FIDIS

Future of Identity in the Information Society

Title:	D11.9: Study on Traffic Monitoring
Author:	WP11
Editors:	Bart Custers, Leo van der Wees (TILT)
Reviewer(s):	Jozef Vyskoc (VaF)
Identifier:	D11.9
Type:	Report
Version:	1.0
Date:	Saturday, 09 May 2009
Status:	Draft
Class:	Public
File:	fidis-wp11-del11.9.traffic_monitoring.doc

Summary

Transport monitoring is a booming area, notably by following vehicles, often for road pricing, but sometimes also for other purposes, such as speeding enforcement, traffic jam prevention, animal-disease spreading controls, and employee monitoring. When introducing traffic monitoring systems, just like introducing any other new technology, the key question is whether this technology achieves its goal and to what extent there are (negative) side effects. This report gives an non-exhaustive overview of traffic monitoring systems being used and/or developed in four European countries: Belgium, Germany, Sweden, and The Netherlands.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	02.03.2008	• Initial release (Leo van der Wees, Bart Custers)
0.2	26.03.2008	• Updates, including contributions Fidis partners (Bart Custers)
0.3	23.04.2008	• Corrections, updates (Bart Custers)
0.4	02.06.2008	• Corrections, updates, new contributions (Leo van der Wees)
0.5	27.06.2008	• Case study Netherlands, corrections
0.6	07.07.2008	• Revised case studies Belgium, conclusions and executive summary
0.7	04.09.2008	• Final remarks authors added
0.8	22.09.2008	• Finalisation of Chapter 6.3
0.9	22.04.2009	• Reformatting and finalizing of the documents
1.0	01.05.2009	• Final version for delivery

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
Executive Summary	Leo van der Wees (TILT)
1 Introduction	Bart Custers, Leo van der Wees (TILT)
2 Traffic Monitoring Systems	Bart Custers, Leo van der Wees (TILT)
3 Normative Framework	Mireille Hildebrand, Els Soenens (VUB)
4 Function Creep	Bart Custers (TILT)
5 Privacy Issues	Bart Custers (TILT)
6 Cases	Belgium: Fanny Coudert, Eleni Kosta (ICRI) Germany: Martin Meints, Maren Raguse (ICPP) Germany: Denis Royer (JWG) Germany: Sirrix Sweden: Simone Fischer-Huebner, Hans Hedbom (KU) Netherlands: Leo van der Wees (TILT)
7 Conclusion	Leo van der Wees (TILT)

Table of Contents

Executive Summary

Transport monitoring is a booming area, notably by following vehicles, often for road pricing, but sometimes also for other purposes, such as speeding enforcement, traffic jam prevention, animal-disease spreading controls, and employee monitoring. This means that vehicles and roads are increasingly equipped with monitoring devices which are used in conjunction with the vehicle ID (number plates). This raises questions on converging technologies, interoperability, profiling, privacy, free movement of goods in Europe, etc.

This study is an inventory on traffic monitoring and has as central research question: "What kind of systems are being used or going to be used in Europe to monitor (road) traffic, how do these relate to mobile identity and profiling, and what normative questions does traffic monitoring raise?"

To answer the first part of the question, this research contains seven case studies from four different countries (Belgium (2), Germany (3), Sweden, and The Netherlands).

The Belgium case studies describe traffic monitoring systems using video surveillance and using floating car data (FCD). The first system is used for detecting road offences, the second for traffic management purposes (crowd control).

The first German traffic monitoring system described also works on the basis of automatic number plate recognition. The same is true for the German system using electronic license plates. In fact this system is a follow-up for the "old-fashioned" ANPR systems using techniques as Optical Character Recognition (OCR). The third German system described is a car telematics system used in some high end cars like BMW. Here of course the vehicle is traceable. That is what is service is meant for.

The Swedish case describes a toll system for Stockholm. This is system is introduced to reduce traffic and to improve the environment. The system uses ANPR technologies to identify the cars (and it´s owners) to be able to charge the taxes to be paid.

The last case study is on the Dutch system called Kilometerprijs. This system also has several goals: traffic management, fair pricing, the environment. The system, to be implemented for heavy vehicles in 2011, uses on board equipment in combination with satellites to follow vehicles and to charge users of the Dutch road system.

Despite the fact that only four countries is being looked at the case studies shows that there is a variety of systems using a variety of technologies. What also has become clear is that traffic monitoring systems (TMS) influence how information available in public spaces is gathered, processed and stored. On the one hand, the efficiency and safety of traffic (monitoring) can justify new information flows but on the other hand, norms of appropriateness and distribution should be respected as well. How can we improve efficiency and safe driving without violating norms of appropriateness and distribution?

In order to do so Hildebrand en Soenens give a non-exhaustive overview of some of the normative questions related to traffic monitoring. They have chosen a broad perspective, using the three principles locality, reciprocity and understanding. This should help to provide a better understanding of how normative issues in this field can be addressed.

What they demonstrate is that answering normative questions on traffic monitoring systems cannot be a straightforward exercise. It depends on a context-specific evaluation of the criteria

of locality, reciprocity and understanding. They also stress that normative challenges of TMSs should be made explicit (and dealt with) as much as possible in the designer phase already.

Hildebrand and Soenens explore normative questions in the domain of traffic monitoring systems that, amongst others, create a tension between the purpose specific use of information flows in traffic monitoring systems and secondary use of (personal) data by third parties, and between privacy of citizens and the need for the transparency of their behaviours.

Those tensions are noticed by the researchers while examining the case studies in the various countries. Therefore, special attention is paid by Custers in his chapters on function creep and privacy.

The traffic monitoring systems described can be used for various purposes easily. The more advanced the system, the more possible purposes. However, if governments want civilians to accept and use the systems transparency is required, especially where the goal of the system is concerned. Using traffic monitoring systems for other means, function creep, does rise several questions. A very important one which almost always is being asked, no matter what type of monitoring system is being used, is related to privacy. But also when traffic monitoring systems are used for the goals they are developed for, privacy issues play a role.

From privacy perspective, systems that process data immediately and do not store them are the most desirable. The data should be stored for as short a time as possible and should not be used for other purposes than the purpose for which they were originally intended. Large central databases are undesirable from a privacy perspective and may also cause maintenance problems. However, other interests may be of more importance than privacy. But, when measures that may infringe privacy are considered, it is recommended that the following principles are taken into account:

- Efficacy: when a particular measure does not contribute to the interest that is more important than privacy, then infringing the privacy is not necessary.
- Subsidiarity: when the interest that is more important than privacy may be achieved in another way, then choose the alternative that infringes privacy least.
- Additional measures: when a particular privacy infringement is considered necessary, take additional measures that limit or compensate the infringement as much as possible.

Although these measures appear to be rather common sense, it is important to note that they are rarely used in practice. Privacy is an interest that should be balanced against other interests.

1 Introduction

Many countries are nowadays using or developing traffic monitoring systems. These systems are in most cases intended to deal with traffic congestion and traffic jams. Also fairer pricing of road use and environmental aspects, including emission reductions, play a role in introducing traffic monitoring systems. And there are many more purposes for which traffic monitoring systems can be used, such as speed checks and criminal investigations. This raises the question for which purposes these systems can and should be used.

When introducing traffic monitoring systems, just like introducing any other new technology, the key question is whether this technology achieves its goal and to what extent there are (negative) side effects. This report gives an non-exhaustive overview of traffic monitoring systems being used and/or developed in four European countries: Belgium, Germany, Sweden, and The Netherlands. Also, normative questions raised by traffic monitoring systems will be described, as well as potential side effects.

After this introduction in chapter 2 technologies used for traffic monitoring are described: Automatic Number Plate Recognition (ANPR), On Board Units (OBUs)[1], and types of communications like Dedicated Short Range Communications (DSRC). Furthermore, is discussed briefly to what extent these systems may achieve goals like fairer pricing, reducing of traffic jams, and environmental improvements.

In chapter 3, a normative framework is provided. This framework contributes to understanding the normative questions related to traffic monitoring. Privacy, autonomy and security are some of the important issues in the design and use of traffic monitoring systems. Furthermore, the principles of locality, reciprocity and understanding are introduced to help providing better understanding of how to address the normative issues.

In order to understand the potential side effects of traffic monitoring systems, chapter 4 provides a more detailed overview of these possible effects. Note that this chapter deals with *side* effects, as the (main) effects that are usually intended by traffic monitoring systems are dealt with in chapter 2. Originally unintended side effects are indicated as function creep. Furthermore it should be mentioned that this chapter deals with *potential* side effects. These effects are often not intended when designing and introducing traffic monitoring systems, but they may come into scope once the systems are being used. Will it be necessary to avoid those effect, and, if yes, how? What kind of technological, legal or organisational measures can be taken to avoid the effects.

Chapter 5 will discuss possible privacy issues that may be raised by the intended effects *and* the potential side effects of traffic monitoring systems. The first focus is on data mining and risk profiling. Aggregated vehicle location data may enable modelling and profiling. This may, however, result in limited reliability of information, stigmatization of particular groups, confrontation with unwanted information and illegitimate selection criteria.

The second focus is on the link between vehicles and natural persons. Mistakes in addressing the wrong person may occur, but also people may use identity fraud to avoid recognition.

The third focus is on limited reliability and interpretations that are incorrect or incomplete. This may result in a privacy paradox, in which people have to provide additional information about themselves when correcting incorrect assumptions that others have about them.

[1] Also refered to as On Board Equipment (OBE)

Furthermore, even though traffic monitoring data may be properly protected, aggregated information, trends and group risk profiles may become known to other parties that may start acting upon this information.

In Chapter 6, seven different case studies are presented. Two Belgium cases of traffic monitoring are described. One on traffic monitoring via video-surveillance and another dealing with floating car data. Three German cases are illustrated. A system using Automatic Number Plate Recognition (ANPR), one on electronic license plates, and a third using car telematics. Next a Swedish system is explained, the Stockholm Congestion Tax System. The last system mentioned is a Dutch system called Kilometerprijs. A system which should be in use in 2011 and which uses satellites in combination with telecommunications to monitor vehicles wherever they are on the Dutch road system.

In the final chapter, Chapter 7, conclusions are provided.

2 Systems for traffic monitoring

Road pricing is an economic concept regarding the various direct charges applied for the use of roads. The road charges include fuel taxes, licence fees, parking taxes, tolls, and congestion charges, including those which may vary by time of day, by the specific road, or by the specific vehicle type, being used. Road pricing has two main distinct objectives: revenue generation, usually for road infrastructure financing, and congestion pricing for demand management purposes. Toll roads[2] are the typical example of revenue generation. Charges for using high-occupancy toll (HOT) lanes or urban tolls for entering a restricted area of a city are typical examples of using road pricing for congestion management purposes.[3] Next to these options European governments are giving serious consideration to nationwide road pricing schemes, because of the ever rising levels of traffic congestion.

For road pricing old fashioned toll boxes can be used but those boxes cause congestions the system actually wants to avoid. Therefore for monitoring purposes more and more advanced technologies are in use or being developed.

Roughly, two systems may be distinguished for determining the uses of roads.[4] The first system uses a network of cameras that automatically recognize number plates. These so-called ANPR systems (Automatic Number Plate Recognition) register at particular locations which vehicles are passing by. The second system uses so-called on board units (OBUs), small boxes that are installed in the vehicle. These boxes monitor which roads were being driven along, for how far and at what time of day. In both situations information of the road use is sent to a central computer system in order to charge the owner of the vehicle.

For communications different systems can be used: Global System for Mobile communications (GSM)[5], General Packet Radio Service (GPRS)[6], Dedicated Short Range Communications (DSRC)[7], or satellite systems like Galileo.[8]

2.1 ANPR[9]

Since the ANPR system relies on a network of cameras registering which vehicles pass by at particular locations, it is possible to charge for particular routes at particular times, for instance a busy ring road during the morning peak hour. It is also possible to demarcate a particular area. This was done for the London congestion charge, where drivers only pay the charge when their vehicle is within the demarcated area in the city center.

---

[2] Toll roads in Europe, Wikipedia <en.wikipedia.org/wiki/Toll_roads_in_Europe>
[3] Road pricing, Wikipedia <en.wikipedia.org/wiki/Road_pricing>.
[4] Road pricing is also possible without any of these techniques, namely by manual declaration by drivers. Since such systems are very susceptible to fraud, they are usually not a realistic option for governments. Manual declaration will therefore not be discussed in this contribution.
[5] GSM, Wikipedia <en.wikipedia.org/wiki/GSM>.
[6] GPRS, Wikipedia <en.wikipedia.org/wiki/General_Packet_Radio_Service>.
[7] DSRC, Wikipedia <en.wikipedia.org/wiki/DSRC>.
[8] Galileo, Wikipedia <en.wikipedia.org/wiki/Galileo_positioning_system>.
[9] Other names are Automatic licence plate recognition (ALPR), Automatic vehicle identification (AVI), Car plate recognition (CPR), Licence plate recognition (LPR), Lecture Automatique de Plaques d'Immatriculation (LAPI).

The ANPR systems are very similar to classic toll systems, in which a vehicle using a particular route is guided through a toll gate where drivers pay a flat fee or collect a ticket that indicates where they entered the highway. In the latter case, there are toll gates at every exit, where the distance traveled is determined and the user is charged accordingly. The problem with these classic toll systems is that traffic flow is limited because every driver has to stop at the ticket booth. ANPR systems do not have this drawback, since determining the location of the vehicle and charging are automated and distance-operated. When vehicles can be charged without having to stop, this is indicated as *free flow*.

The major advantage of ANPR is that the investments are relatively low. With the use of cameras and software that can recognize number plates, such a system can quickly be built. It is easy to start on a small scale, for instance, on one or two routes, and then roll out the system. Another advantage is that the system can be used rather easily for vehicles from other countries.

The disadvantage of ANPR is that it cannot be used for road pricing in a whole country. After all, for that it would be necessary to place ANPR camera´s along all roads and crossings which is not only expensive, it would also spoil the landscape. And when camera´s are placed along main roads only, drivers may avoid registration by using secondary roads. On the other hand, the question is whether every kilometre travelled should be charged. It may be sufficient to charge only for congested routes during peak hours, as is done in London and Stockholm. Hence, this system can only realize some of the purposes of road pricing, since there is also use of (secondary) roads and pollution of the environment that is not charged for. Nevertheless, ANPR is an adequate solution for reducing traffic jams, if congested routes are monitored and sufficiently charged for. It remains to be seen whether ANPR will really solve all traffic jams, but the system at least addresses this problem. When the price for particular routes increases, fewer drivers will choose to use these routes. The question is how high the price has to be, to solve traffic jams and whether these prices are still acceptable.

Concerns about these systems have centered on privacy fears of government tracking citizens' movements and media reports of misidentification and high error rates. However, as they have developed, the systems have become much more accurate and reliable.[10] For more information on privacy and ANPR see the German case study on Automatic Number Plate Recognition.

The cloning of number plates, already encouraged in London by the Congestion Charge, is also likely to increase as a consequence of ANPR, making life difficult, possibly hazardous, for the owners of the vehicles cloned.[11] In other words, ANPR might give a boost to incidents of identity fraud.[12]

---

[10] See Automatic number plate recognition, Wikipedia <en.wikipedia.org/wiki/Automatic_number_plate_recognition>.

[11] No hiding place? UK number plate cameras go national, The Register, 24 March 2005, <www.theregister.co.uk/2005/03/24/anpr_national_system/>.

[12] Identiteitsfraude, Justitiële verkenningen, 7/06, Dutch text and English summary available at <www.wodc.nl/onderzoeksdatabase/jv200607-identiteitsfraude.aspx>.

2.2 On Board Units

Systems with On Board Units (OBUs) are based on installing a box or equipment in the vehicle with a unique identification facility that can be detected by or make contact with a satellite or detection systems along the road. A much used technology in this box is RFID (*Radio Frequency Identification*). This technology enables storing and processing information of so-called *RFID tags*.[13] Passive tags have no battery and cannot store information; they can only reply to inquiring signals by deforming them. These tags are often used in access tokens, e.g., for entering buildings. Active tags are equipped with a source of energy. Information on these tags can be stored and processed from a distance. Passive RFID cannot store the location of the vehicle in the OBU. Determining the distances travelled has to take place elsewhere, for instance, by using a system that is coupled to transmitting antennas. Communication with the OBU can also take place in other ways, for example, by using a navigation system, such as GPS.

The advantage of OBUs is the high accuracy in determining the location of a vehicle every moment in time. Particularly systems using satellite navigation cover road networks of entire areas. The coverage of a ground network is no longer relevant in such cases. Such accurate location data may be used for fair pricing and more personalized pricing: every piece of road may be charged at a different price at a different time.

The advanced accuracy of these systems causes disadvantages as well. From a privacy perspective, more information is available and this information can be used or abused more frequently and more easily. This will be discussed further below. Furthermore, collecting and processing large amounts of data does not only raise privacy concerns, but also concerns regarding efficacy and efficiency. Large amounts of data may result in loss of overview and lead to significantly increased processing times. Another disadvantage of OBUs is the relatively high costs of equipping every vehicle with this technology. This may also lead to resistance of drivers who do not want to cooperate with installing technology that is used for charging them. Furthermore, this system is not ideal in an international context, as foreign vehicles may not have OBUs and will have to be charged in other ways.

2.3 Communications

For ANPR camera´s are used to take pictures of the license plates of the vehicles using particular roads. Often pictures are taken of vehicles of the front and the rear plate, and when entering and when leaving an area resulting in higher chances to register a vehicle. After the picture has been taken the images are being send to a data centre for processing and, in the end, charging the owner of the vehicle. So there is a (cable) connection between camera´s and data centre.

Using On Board Units various ways and sorts of communications are possible. When OBUs are used for electronic toll collection systems using toll gates often dedicated short range communications (DSRC) is used to let the OBU - often a transponder – communicate with the gate and the toll collecting system. DSRC is a short to medium range wireless protocol specifically designed for automotive use. It offers communication between the vehicle and roadside equipment. It is a sub-set of the RFID-technology. This technology for intelligent

[13] For more detail, see also FIDIS report 11.9: Royer, D., et al. (2008) Study on Mobile Identities for Transport Monitoring.

transportation system (ITS) applications is working in the 5.9 GHz band (U.S.) or 5.8 GHz band (Japan, Europe).

OBUs used for road pricing systems can also communicate with satellites like the Galileo satellite positioning system. In that case short range communications will not suffice to follow vehicles. Other communications protocols will be used then, like Global System for Mobile communications (GSM) and General Packet Radio Service (GPRS). GSM is the popular communications standard for mobile phones, and GPRS is a newer version of that standard which added packet data capabilities to it.

2.4 Goals

Once the location history or distance travelled by a vehicle is determined, the rates can be determined and charged. The flexibility of pricing depends on the system chosen for traffic monitoring. If a system only registers the distance travelled, then the only parameter for pricing is that particular distance. This may result in pricing per kilometre or mile, but also at fixed rates per 10,000 kilometres. In this way, everyone driving between 10,000 and 20,000 kilometres will pay the same charge, but people driving between 20,000 and 30,000 kilometres will pay the higher charge. The first 5,000 kilometres may be free of any charge. Rates may be proportional to the number of kilometres, but may also increase exponentially.

When only the distance travelled is known, it is impossible to charge extra for using particular routes at specific times. Hence, any incentives for road users to avoid particular roads during peak hours are very limited. A more advanced system for road pricing needs more parameters.

More parameters for pricing can only be used when the traffic monitoring system registers the location history of a vehicle and also data of the vehicle itself, like weight, size, and type of fuel used. Using these data, it is possible to charge not only for the distance travelled, but also for using particular routes during particular hours. This enables addressing traffic jams in addition to road use and environmental impact. The basic assumption is that seriously charging routes with a lot of congestion may cause people to look for alternatives, such as travelling at other times or using public transport. Location data available for every moment in time can be used for creating a pricing model. This also enables introducing benefits and discounts in the model, e.g., for persons avoiding peak hours, for always using the same route, or driving particular cars.

Whether or not the goals of the various pricing mechanisms will be achieved is hard to predict since there aren´t that many examples worldwide. The toll system in Stockholm seems to be quite successful. It has been said that just after the introduction of the system in August 2007 there was a reduction of traffic of 25%. Next to that there was an increase in sales of cars less harmful for the environment, because owners of those cars exempted from paying toll.[14]

Outside Europe especially Singapore seems to be a success story, but not only because of the road pricing system. Is seems to be the result of a variety of measures: high annual road tax, custom duties, fuel taxes, high parking rates, next to congestion charges. Apart from that the Singapore government has invested heavily in public transportation and implemented a park-and-ride scheme. Singapore's urban and transport strategy allowed users to have pro-transit

[14] Zweedse tol als succesvoorbeeld, De Pers, 13 mei 2008

"carrots" matching auto-restraint "sticks".[15] As a result, and despite having one of the highest per capita incomes in Asia, fewer than 30% of Singaporean households owns cars.

[15] Robert Cervero, Chapter 6/The Master Planned Transit Metropolis: Singapore, The Transit Metropolis, Island Press, Washington, D.C., 1998.

3 Normative Questions

3.1 Introduction

This contribution provides a non-exhaustive overview of some of the normative questions related to traffic monitoring. Instead of focusing our attention exclusively on the issues of privacy, autonomy, we have chosen a broader perspective, using the three principles of (Roussos, Peterson et al. 2003), locality, reciprocity and understanding. This should help to provide a better understanding of how normative issues in this field can be addressed.

3.2 Traffic monitoring

Traffic monitoring involves a broad field of techniques which all relate to profiling. Traffic Monitoring Systems (TMSs) profile vehicles and/or other objects for road network performance (crowd and flow control and planning interventions), for congestion charges (London), for registration of evidence in case of traffic rule violations, for calculating travel times or for electronic toll collection. Recently the use and development of 'Intelligent Transportation Systems (IST)'[16] has been booming (El Faouzi 2006). Traffic monitoring relies on a broad scope of data types from various sources. Data fusion of Radio Frequency Identification (RFID), Smart cards, Closed Circuit Television (CCTV), Remote Traffic Microwave Sensors (RMTS) etc. all enable traffic monitoring.

The implementation of smart technologies in cars implies that cars actually become *active* messengers: they are not only seen but see as well, they are not only detected but detect as well. Traffic monitoring systems make clear that objects can be what (Latour 1987) called *actants* (non human actors) in (socio-technical) environments.

3.3 A normative point of view on Traffic Monitoring Systems

Normative questions

It is of major importance to explore the normative issues raised by new technologies. Normative reflections emphasize the significance and consequences of (often tacit) choices that are made in the design of the system. In a democratic society, the balancing of values is essential. This also means that in one way or another, equilibrium should be maintained between (sometimes contradicting) ethics and standards. In the case of traffic monitoring systems, we see several (interrelated) tensions.

[16] 'Intelligent Transportation Systems (ITS) is a broad range of diverse technologies applied to transportation to make systems safer, more efficient, more reliable and more environmentally friendly, without necessarily having to physically alter existing infrastructure. The range of technologies involved includes sensor and control technologies, communications, and computer informatics and cuts across disciplines such as transportation, engineering, telecommunications, computer science, finance, electronic commerce and automobile manufacturing': <www.its-sti.gc.ca/en/what_is_its.htm>.

A first normative question addresses the balance between the **privacy of citizens and their transparency for the sake of holding them accountable in the case of harm caused**. On the one hand, privacy is a fundamental human right, but on the other hand, it is no absolute right. It can be limited e.g. for reasons of public interest in a democratic society. Depending on the specific public interest (efficient traffic flows; the penalization of speed drivers and car thieves etc.) potential privacy intrusions have to be evaluated. This issue also concerns the need for transparency of government bureaucracy, as regulated in e.g. the data protection directive D46/95/EC, which is related to what has been called the reciprocity principle (see below at section 3.4.2).

A second normative issue relates to the tension between **individual human autonomy and technologically induced or even enforced actions and behaviour patterns**. Throughout history we see that conformity to (what is defined by society as) acceptable behaviour and social norms has been marked out by technology.[17] To some extent, social control has increasingly been determined by technological systems and this is initiated both by public *and* private actants. As a result, citizens may be put in the position of no longer having any real self-determination, for instance when driving a car.

The two normative questions above are strongly related. Privacy protection, as an opacity tool, enables human autonomy and self-determination in social life – whereas transparency (of citizen's behaviour) can be essential when making '*actants'* accountable for their actions. If we value privacy, this does not mean transparency should be neglected as a public good. The question is 'what is the demarcation line in the case of TMSs'? To what degree should individual human autonomy be preserved? Which technical actions and measures should be tolerated for the sake of the public good of accountability?

Another normative issue concerns machine-to-machine communication (M2M talk) and human-machine interfacing (HMI). These are essential features in the domain of traffic monitoring that stress the significance of non-human actants because of their normative impact. Many questions need to be addressed regarding **causality, responsibility and – legal - liability**, e.g.:

- Who will be made responsible for an accident in case a driver neglects the instructions of an intelligent transportation system?
- Can we assume that all consequences of the behaviour of the traffic monitoring system have been intended?
    - If so, by whom or by what?
- What if the influence of the traffic monitoring system is so strong that the technological system prevents the driver from exercising human discretion?

Related to the latest question we can think of scenarios in which individual autonomy and/or individual responsibility is limited by technologically embedded scripts. In other words, socially correct behaviour and social control is being pushed by technology rather than by human discretion. For instance, imagine that, in an ambient intelligence (AmI) environment, traffic monitoring systems are able to automatically limit the speed of cars because of high CO2- pollution levels. Now traffic signs invite drivers to limit speed and when they do not

[17] For example: Stealing of property has been prevented by keys and alarm systems.

comply they can be fined. Individual freedom as well as individual responsibility are essential for behaving oneself in traffic. But when traffic monitoring systems have the ability to limit cars' speed automatically, responsibility seems to be taken away from the individual by embedding social control in the technology.

How to evaluate normative aspects?

The evaluation of normative aspects of traffic monitoring systems is of course very case-specific. The evaluation depends e.g. on the purposes of the system in use, the kind of profiling that is done (e.g. the norm against which the actant is checked) as well as how the location and other data is dealt with.

The first difference between alternative TMSs concerns the **purpose** of the system in use. The case studies in this deliverable show a variability in rationales. Some TMSs are (can be) explicitly used for road toll systems (cases: Brussels urban toll project, the Stockholm Congestion Tax System). Others concentrate on traffic speeding and crowd control (case: Floating Car Data (FCD) project in Flanders). Still others are used for identification of road offences (case: Belgian Video Surveillance case) or tax control offences (case: German case). And the Dutch system of Kilometerprijs intends to add environmental goals to the system which also made for fairer pricing of road use and crow control.

In relation to the purpose specifications, TMSs also differ in how the driver (or car) is 'known to the system'. In general, there is a substantial difference between TMSs that focus on re-recognition and those that enable the identification of the driver (or car) (Dötzer 2005). Re-recognition is defined as 'keeping identifiers and relating them to other received identifiers', while identification is defined as 'correlating the identifier with a real-world identity'. This means that re-recognition is possible without identifying the person 'behind' the identifier. Privacy protection is served by re-recognition without identification, while accountability requires identification. The right balance depends on the purpose of the system. Identification is necessary, e.g. in the case of security issues or when violations against traffic rules are fined (e.g. ICRI case traffic monitoring via video surveillance: cameras with identification purposes mainly used for the detection of road offences). Re-recognition is sufficient e.g. in the case of media and entertainment or traffic road information, in which case the point is that 'messages reach their destination(s)', which is also called addressing. Also, when the TMS is designed to simply monitor traffic, e.g. in the Floating Car Data in the Flanders project, anonymous data should be used guaranteeing that the identification of the driver is impossible. After all, identification is not necessary to serve the goal of the system. However, since the project makes use of ('anonymous' traffic and location) data collected through mobile phones in the cars, identification of the data is easily done and the data should be treated as personal data. In other words, the design of the system causes it to process more data than needed for the purpose of the system.

Besides the purpose specification, there is a second substantial difference that is relevant in the case of traffic monitoring. This is, what (Müller and Boos 2004) call the **norm against which an actant is checked**: e.g. an individual marker, or behavioural markers. In the case of individual markers an individual actant is identified or re-recognized by means of individual markers, registered in a data base, e.g. in the case of charging congestion charges. In the case of behavioural markers actants are matched on the basis of algorithms against a defined

'normality' (Müller and Boos 2004), at 13), e.g. in the case that slower driving at a certain point would improve the traffic flow.

A third difference between alternative TMSs concerns **the way they deal with location and other identity related data**, as this also influences the normative analysis. There is an important difference between data that is merely used to be checked against information in other databases (e.g. in the Stockholm Congestion Tax System: in general the data is deleted 28 days after payment) and data that is also used to create new databases (e.g. the Belgian law proposal to create 'an authentic source of data relative to vehicles').

In the case of the Floating Car Data in Flanders, the role of commercial services in the use of traffic data for traffic monitoring systems is discussed. According to article 4 (1) of the Belgian data protection law, further processing of data is allowed without providing additional reasons if the data are further processed 'in a way compatible with the initial specified, explicit and legitimate purposes' (cf. art 6 (1) (b) of D/95/46/EC).

Discussion on the allowance of commercial services – value added services - to be provided using the data of the on board equipment used for the system of Kilometerprijs also takes place in The Netherlands. The idea behind the provision of such services is that this might reduce the price of the on board equipment as well operating costs. In this framework it is also kept in mind that vehicles will have on board equipment anyway in the near future. This means that if an open standard for equipment is provided space is created for commercial parties to supply equipment as well. This equipment, however, should meet certain standards because of which the idea of a certificate has risen. Of course the equipment should be able to be interoperable with the system of Kilometerprijs. It is however thinkable that it is also required that the equipment has the possibilities for users to block and un-block commercial services if added to it, resulting users to be left alone if they want to and resulting in a system compliant to anti-spam rules.[18]

A fourth difference relates to **secondary use of data**, as this may result in illegitimate data processing. The German case on ANPR addresses this inquiry in the paragraph on legal aspects of heavy vehicles toll collection. Especially when "strict and exceptionless purpose binding"[19] provisions exist as is the case in the German Motorway Toll Act (Article 4 section 2 sentence 3), it should not be allowed to use data collected and processed for toll collection for other purposes, e.g. by enforcement authorities. We should be on the alert for function creep (see chapter 4), which could occur when country courts frequently decide to overrule the toll act or when amendments to the relevant statutes are made to legalise the secondary use of traffic and other data.

[18] Starten met de kilometerprijs. Overzicht van voorbereidend onderzoek bij het kabinetsbesluit over de kilometerprijs., Ministry of Transport, Public Works and Water Management. The report is available on the website of the ministry, <www.verkeerenwaterstaat.nl>. Click *Mobiliteit en bereikbaarheid* and next click *Anders Betalen voor Mobiliteit*.

[19] Schäuble, W., 2007, *Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts*, Zeitschrift für Rechtspolitik No. 7/2007.

3.4 How to address normative issues in traffic monitoring systems

Privacy implications, assaults on human autonomy and the level of transparency all depend on the choices made *in and through* the design[20] and the use of the technological system in question. However, there are no straightforward, definite answers to this matter. In this section we will demonstrate how the principles of *locality, reciprocity and understanding*, introduced by (Roussos, Peterson et al. 2003) in the context of mobile identity management, may clarify the normative issues that are at stake. Hereunder we briefly introduce these principles, also referring to FIDIS Deliverable D11.1, at section 4.5.2.

3.4.1 The locality principle

(Roussos, Peterson et al. 2003, 94), state that, 'identities are situated in particular contexts, relationships, roles and communities, and that we may have different or overlapping identities attaching to different contexts.' This compares well to (Nissenbaum 2004, 118-9), who developed the notion of 'contextual integrity', rejecting

- 'a universal account of what does and does not warrant restrictive, privacy-motivated measures, in order to take into account dimensions of time, location and so forth' and
- 'a right of privacy [expressed, mh] in terms of dichotomies - like sensitive and non-sensitive, private and public, government and private – that line up, interestingly, with aspects of the general public-private dichotomy that has been useful in other areas of political and legal inquiry. That which falls within any one of the appropriate halves warrants privacy consideration; for all the rest, anything goes',

while advocating that

- there are no arenas of life not governed by norms of information flow, no information or spheres of life for which 'anything goes';
- information flows should be regulated by
    - norms of appropriateness (e.g. what is allowable, expected or even demanded to be revealed in a specific context) and
    - norms of distribution (e.g. free choice, discretion, confidentiality, need, entitlement and obligation) (Nissenbaum 2004), 119-125).

In other words, Nissenbaum develops a response to the fact that information technologies have blurred the borders between the public and the private. In her opinion the need for the protection of one's integrity can no longer be resolved by a one-sided emphasis on privacy in the sense of non-disclosure of personal data pertaining to the private sphere. Instead of thinking in terms of neatly separated private and public spheres in relations to the

[20] The 'value-sensitive design' or 'values in Technologies' perspective. This perspective wants to emphazise the (social, political, ethical) value implications inherent in the design of new ICTs. For more information see <www.nyu.edu/projects/valuesindesign/index.html>. See also Friedman, B., *Value-sensitive design: a research agenda for information technology*, National Science Foundation, Aelingotn, VA., 1999.

transparency of citizens, she advocates an analysis that is more sensitive to the appropriateness of data sharing in a variety of contexts (localities), while discriminating between different ways of distributing. This means we may have to develop legal and technological infrastructures to protect our privacy in public.[21]

In a recent article, (Zimmer 2005) made use of the contextual privacy framework of Nissenbaum to enhance awareness in the design community of the ethical implications (such as mass surveillance) of vehicle safety communication (VSC)[22] technologies. He stresses that traffic-monitoring systems bring about the risk of threatening *privacy in public* because these systems no longer follow the traditional norms of distribution and appropriateness as they existed in the anonymous context of the highway. The Vehicle Identification Number (VIN) and e-license plates (see e.g. the German case on mobile identities and electronic license plates) deprive drivers of the level of privacy in public they have been used to. As a result of TMSs, highways - classical islands of anonynimity - will become less and less a context in which you can enjoy privacy in public. Zimmer's evaluation of the consequences of VSC technologies on contextual privacy is useful to raise awareness for value-in-design methodologies.

The locality principle stresses the urge to design TMSs in ways that take into consideration the various specific contexts in which people behave. Consequently, a centralized system which works with one overall identity, contradicts the principle of locality. Therefore, decentralisation of the various layers of the TMSs is to be preferred. (Dötzer 2005) describes so-called Vehicular Ad Hoc Networks (VANETs), which are 'self-organizing and decentralized', enabling both secure and privacy friendly monitoring. They achieve this by means of decentralized, car-to-car communication, which means that no data are stored in a central data base. Although connections to central authorities may not be completely inevitable, it seems that from a privacy and security point of view TMSs which work with peer-to-peer communication are to be preferred above systems which use centralized communications (cf. (Harmon, Marca et al. 2006). However, in case of the Brussels Urban Toll Project, which discusses the secondary effects of decentralized communications in Traffic Monitoring Systems, it turns out that, although (centralized) ANPR (automatic number plate recognition) implies automatic recognition software and the creation of other databases as well as the processing of location data, it could still be less privacy intrusive than the DSRC (Dedicated Short Range Communication) technologies which are mostly embedded in decentralized communications networks. The reason for this is that in the case of the Brussels Urban Toll Project the ANPR, as described by the report issued by Inter-Environment Bruxelles on the topic, would not register the movements of drivers (see the Belgian case on traffic monitoring via video surveillance).[23]

---

[21] The adjective 'public' can refer to the publicness of a context or to its governmental nature. Being out on the street we are in a public space, which is not necessarily a governmental space. Public law, however, usually refers to the laws that regulate governmental competences.

[22] VCS technologies 'combine intelligent on-board processing systems with wireless communications for real-time transmission and processing of relevant safety data to provide warnings of hazards, predict dangerous scenarious and help avoid collisions: Zimmer, (2005, 2) Most of these VSC techniques are still in development phase.

[23] Inter-Envrionment Bruxelles is an organisation that federates more than 80 neighborhood associations and specialized group, and aims at improving life quality in Brussels. More information can be found at www.ieb.be (in French). The report follows a debate organized on the 20th November 2007 on the benefits and drawbacks of

The locality principle is explicitly at stake when identifiers essential to the traffic monitoring system are used for (secondary) purposes. For example, in the ANPR case, it is mentioned that 'the relevance of ANPR for the subject's personality can increase depending on the location ANPR is used at, and which further information the police holds about data subjects if number plate recognition is indirectly used to analyse the passengers' other behaviour (e.g. participation in political marches). Also, whenever ANPR data is used for further matching with other databases and creation of movement profiles, the locality principle is at stake.

In sum, the locality principle addresses the concern that privacy preferences change depending on a person's role and context. For this reason traffic monitoring systems should be designed to guarantee flexible changes in privacy parameters. For instance, privacy friendly solutions could be guaranteed e.g. by the use of what (Dötzer 2005) calls Geo Bound Pseudonyms, used for the purpose of re-recognition: 'That means for every geographic position there is a set of associated pseudonyms available, being a true subset of all pseudonyms used by that single vehicle'.

3.4.2 The reciprocity principle

In relation to the reciprocity principle, (Roussos, Peterson et al. 2003, 95) explain that

- this principle bears primarily on issues of privacy, profiling, and surveillance, and implies that collecting identity data by tracking the activities of individuals will be unacceptable if it is not reciprocal
- a relationship is nonreciprocal and asymmetrical if one does not know who is collecting the data, how the data will be used, how to corrects errors in the data and whether to expect a return.

It is assumed that 'both sides in a relationship need to know what is going on so that they can check and correct each other's perceptions' (Roussos, Peterson et al. 2003, 94). This principle relates to the need for *mutual* transparency in the use of new technologies. In fact, people are used to making decisions based on imperfect information. In their report on a wireless P2P network for roadway incident exchange (Harmon, Marca et al. 2006) explain how a decentralized network provides 'vehicle to vehicle exchange of information related to conditions that the traveller does not know', thus enabling increased transparency that nourishes reciprocity. One can also point to (Jiang 2002)'s principle of minimisation of information asymmetry, that seems to confirm the importance of the reciprocity principle, perhaps providing a more feasible target. Interestingly this principle directs the attention from data minimisation as a goal in itself (focus on opacity), to minimisation of asymmetry, which aims to create a balance between the knowledge of interacting persons (focus on mutual transparency).

In this context, it is interesting to remark that several authors of the case studies mention the lack of information about the TMSs: 'no detailed information about the project, and about the floating vehicle technology software developed by ITIS holdings plc is available' (see the

---

the introduction of a urban toll in Brussels to reduce traffic congestion. More information (in French) can be found at <www.ieb.be/article/843/>.

Floating car data case (see the second Belgian case), and 'the information available from [BMW2008] does not contain any hint on any use of special technology for special handling of location data to provide privacy to the car's users' (see the third German case on the BMW ConnectedDrive car telematics service). These are examples of systems that seems to violate the principle of minimal data asymmetry and the principle of reciprocity.

Interestingly, the case on Automatic Number Plate Recognition (the first German caseP) indicates that the principle is reflected in German case law: 'in the case of surveillance measures the principle of certainty requires that the data subject can realize on which occasion and according to which requirements a certain behaviour will result in the threat of surveillance.[24],

In emphasizing the reciprocity principle, designers of TMSs could be made aware of the negative effects of the proliferation of surveillance systems. In this respect, the Australian New South Wales Privacy Committee (1996-7, 15, cited in (Fox 2001)) warns for a situation in which the relationship between those actants watching and those actants being watched, produces 'an asymmetry of knowledge and consequent imbalances of power'.

3.4.3 The principle of understanding

This last principle points out to the fact that 'identity serves in two-way relationships as a basis for mutual understanding' (Roussos, Peterson et al. 2003, 94). Mutual understanding

> 'frequently involves what psychologists call 'simulation': the ability to see things from the point of view of another agent. If the materials for this understanding are not provided, trust and consequently mobile business may suffer' (Roussos, Peterson et al. 2003, 95).

Traffic monitoring systems depend not only on machine-to-machine (M2M) communication, but also on **human-to-machine interfacing (HMI)**. TMSs try to simulate the viewpoints of a diversity of human drivers, but it may be even more difficult to imagine a human person trying to simulate the viewpoint of the machine. Precisely for this reason, the principle of understanding discloses the need for good human-machine-interfaces (HMIs). Indeed, the interpretation of the guidelines of the traffic monitoring system by the driver is not always self-evident. For this reason a user-friendly design of the devices, as well as a design process which is effectively tested in real life situations are of great importance. (Harmon, Marca et al. 2006) stress this point, and include a 'hardware-in-the-loop experiment' in their prototype field implementation experiment, moving from simulation of ad-hoc wireless networks to the real world. This enabled them to assess the current commercial off-the-shelf technologies (COTs), providing 'working protocols and communication parameters for improving future large-scale simulation studies.[25]

[24] BVerfG, NJW 2005, 2607

[25] For a critical perspective on the risks related to security of COTS see: Longstaff, T.A., et al. 'Are we forgetting the risk of COTS Products in Wireless Communications?', Risk Analysis Vol 22, No. 1, 2002.

A problem with existing TMSs is that the design often has roots in non-civil contexts, such as the military. These technologies are then 'transported' to civil society, without much testing of people's understanding of the workings and consequences of those systems.[26]

3.5 Conclusion

Traffic Monitoring Systems influence how information available in public spaces is gathered, processed and stored. Such systems have an impact on existing information flows. On the one hand, the efficiency and safety of traffic (monitoring) can justify new information flows but on the other hand, norms of appropriateness and distribution should be respected in order to guarantee citizens' *privacy in public*. How can we improve efficiency and safe driving without violating norms of appropriateness and distribution? Traffic monitoring systems have the capacity to influence privacy as well as human autonomy. The way in which 'social' control of drivers and roads is technologically mediated, can indeed limit human autonomy in public: 'by conditioning to conformity as well as by the deterrent effect of potential exposure' (Fow, 2001: 268).

In this contribution we stress that - agreeing with the values-in-design perspective - normative challenges of TMSs should be made explicit (and dealt with) as much as possible in the designer phase already. We have explored normative questions in the domain of Traffic Monitoring Systems that create a tension between:

- Privacy of citizens and the need for the transparency of their behaviours
- Individual human autonomy and technologically induced/enforced behaviour
- Legal liability of human and non human actants
- Purpose specific use of information flows in Traffic Monitoring Systems and secondary use of (personal) data by third parties.

Using the principles of Roussos et al., we have demonstrated that answering the normative questions on Traffic Monitoring Systems cannot be a straightforward exercise. It depends on a context-specific evaluation of the criteria of locality (including Nissenbaum's notion of contextual integrity), reciprocity (minimal information asymmetry) and understanding (HMI). Traffic Monitoring Systems could be normatively justified if the value-in-design methodology is used in a way that meets the principles described in this contribution.

[26] See e.g. Harris and Harris, ' Evaluating the transfer of technology between application domains: a critical evaluation of the human component in the system', Ttechnology in society, vol. 26, nr. 4, November 2004, Pages 551-565.

4 Function creep

The traffic monitoring systems described in the previous chapters and in the case studies below can be used for various purposes. The more advanced the system, the more possible purposes. However, if governments want civilians to accept and use the systems transparency is required, especially where the goal of the system is concerned.

It seems that the more technically advanced a system is, the more possibilities do exist for other use than the initial one. The fact that various options do exist, does rise several questions. A very important one which almost always is being asked, no matter what type of monitoring system is being used, is related to privacy.

In order to determine the privacy issues of traffic monitoring, it is essential to understand the intended and unintended possibilities of such systems. Any unintended possibilities may have significant consequences, as applications of new technologies often change after some time. Examples that may illustrate this are cell phones that are currently used for sending short email messages and even for accessing the Internet. Other examples are teletext on TV or bank cards equipped with e-money facilities.

4.1 Speed checks

One of the most controversial applications of traffic monitoring based on location history is the possibility of ascertaining speeding. When a particular vehicle is located at 8:00 am in Amsterdam and 180 kilometres further at 9:15 am, the vehicle must have exceeded the maximum speed at some time. The driver may be fined automatically.

Using a system based on location history, a vehicle may be checked for speeding at any time or location. Obviously this type of speeding checks is impossible when traffic monitoring systems are used that only determine the distance travelled.

Since many road users speed sometimes, the resistance against ticketing minor speeding offences is much larger than against flagrant speeding offences. It is likely that there is a similar resistance against (permanent) speed checks based on traffic monitoring

4.2 Parking checks

Another possibility of traffic monitoring based on location history is executing parking checks. Once it is determined how long a vehicle has been standing at a particular location, it is easy to check whether that was legal. Such parking checks may include whether the time at that location was paid for and checking whether that location was a legal parking location.

Parking permits no longer have to be distributed on paper. Paying other parking fees may also take place via OBUs. Illegal parking may even become impossible. Paying in advance is also possible. The ticket machine may have to be coupled with the OBU for this, in order to determine whether the parking time that has been paid for has been exceeded. Obviously a traffic monitoring system that only determines the distances travelled may offer only few or none of these possibilities for parking checks.

4.3 Traffic information

Data that represent the location of a vehicle may also be used for traffic information. This mainly concerns traffic accidents and traffic jams. The vehicle may be involved in a traffic accident if it has not moved for some time on a location where it should be moving, such as on a highway. The registration system may use pattern recognition for this. In the event of a traffic accident, there will typically be many vehicles behind the location of the accident and only a few in front. Many vehicles in a particular location may indicate a traffic jam. Furthermore, vehicles taking an exceptionally long time for a particular distance may indicate something strange, such as a traffic jam or a car breakdown.[27]

When someone calls the emergency number and provides information on the number plates of the vehicles involved and these vehicles have an OBU, the exact location of the traffic accident may be determined. Emergency services may then quickly be at the location. Furthermore, vehicles that were near the accident may be traced. The drivers of these vehicles or their passengers may be witnesses or suspects (see next subsection).

The length and location of traffic jams may be determined more quickly and accurately. It is even possible to adjust pricing to the current traffic jam situation. Someone who decides to take a particular route on which a traffic jam was announced may be charged extra. For environmental tax purposes, quota may be imposed, for instance, for particulate emission. When the limit is approached, the charges may be increased further to stimulate the driver not to exceed the limit at a particular location.

4.4 Criminal investigation and prosecution

The location history data of vehicles may be used for numerous criminal investigation and prosecution purposes. When a criminal offence has taken place somewhere, the police may investigate which vehicles were near the crime scene at that time. Among this group there may be witnesses, perpetrators or victims who may be of interest for the criminal investigation.

Another application is the tracing of stolen vehicles. If a theft is reported quickly after it has taken place, the vehicle may easily be traced. Even if the vehicle has left the country, there will be data on where it passed the border, which may provide indications about the perpetrator. Vehicles that were stolen abroad and transferred to or via a country may also be traced using traffic monitoring systems based on number plate recognition. If more countries use such systems, cooperation may lead to a better crime solution rate.

Traffic monitoring systems may also help against mobile banditry. Mobile banditry concerns international criminal organizations, particularly from Eastern Europe, that commit a series of crimes, such as robberies, thefts and even liquidations, in another country and leave for their home country immediately afterwards. The vehicles used by these criminal organizations may be (one of the few) leads for solving such crime.

Using the location history of vehicles for criminal investigation purposes does not have to be based on a criminal offence known by the police: the location data may indicate that an

[27] A commercial system using location data of mobile phones of motorists already exists. See: TomTom launches Traffic information based on GSM data, GPS Business News, 12 November 2007 (<www.gpsbusinessnews.com> search for *tomtom launches gsm data*).

unreported crime has taken place. For instance, when a vehicle was at an unusual location for a long time, this may be a reason to investigate what happened at this location. A vehicle that was in the forest during the night for several hours for the first time in twenty years may be reason for the police to have a closer look at this location.

Particular combinations of vehicles owned by people with a criminal record that are always together at the same wayside restaurant or service area may be a sufficient reason for the police for further investigation. The next section will deal in more detail with data mining and risk profiling, techniques for analyzing information that may yield indications about suspect vehicles, persons or locations or combinations of these aspects.

There are many more criminal investigation purposes of traffic monitoring. Vehicle location data may then be used on a larger scale to provide evidence in a court of law. This is similar to the use of location data of phone calls (data retention) as evidence. Phone calls may also indicate the location of a person at a particular time. Obviously it is possible that someone other than the registered owner has used the phone or the vehicle, in which case supporting evidence or an additional explanation may be required. When the linking of persons to vehicles is incorrect, this may indicate identity fraud (see next chapter).

4.5 Scientific research

Vehicle location data may also be used for scientific research, for instance, on the problems regarding traffic jams or the effects of road blocks for road maintenance. This may yield a more accurate picture of the effects of detours, suggesting measures to further minimize any congestion.

Another application would be to survey road users about their satisfaction with, for example, traffic control. The Dutch government sent a letter to road users asking them to complete a questionnaire on this topic. Their names had been selected with cameras that had been registering number plates during two months during traffic jams. From these data it was easy to select the frequent users of that particular route.

4.6 Conclusion

Traffic Monitoring Systems are often designed to perform a certain task, e.g. road pricing. It seems, however, that traffic monitoring systems can perform a variety of tasks next to the initial one. Tasks which might have an impact on privacy. After all, if a system which is designed for road pricing processes personal data which are also given (under conditions) to authorities for criminal investigations or used for research to traffic flows more persons will have access to the personal data and as a consequence chances on abuse of the personal data are higher.

This use of technology for other purposes that the initial one - function creep - is one of the characteristics of what the Dutch Data Commissioner calls the *glass society* with all dangers

thereof.[28] Next to this, function creep might have it's consequences on the use and acceptance of, and trust in traffic monitoring systems.[29]

[28] Kohnstamm, mr. J., dr. L.Dubbeld, Glazen samenleving in zicht, Nederlands Juristenblad, 2007
[29] See for more information on trust in a digital environment Trust in Electronic Commerce, J.E.J. Prins, et al, Kluwer Law International, 2002, and deliverable D17.4 on trust in the light of virtual persons.

5 Privacy issues

It may be questioned whether all the possibilities of using location history data of vehicles mentioned above should be aspired to, as these applications may have different pros and cons. In this section, the drawbacks of the applications mentioned will be described. These drawbacks need not be a reason to cancel all means of traffic monitoring, but they should play a role in considering the way in which traffic monitoring systems are introduced. Smart choices will avoid or minimize the privacy issues discussed below. Furthermore, it is often possible to take additional or compensating measures when particular individuals experience privacy violations or injustice.

5.1 Data mining and risk profiling

The storage of data is controversial subject in the debates on traffic monitoring, as the storage has large impact on the processing possibilities of data and the privacy resulting from it. Different storage aspects that affect the level of privacy are, among other things, the amounts and types of data stored, the duration of storage and the type of storage (central or local). Privacy risks increase in a system in which amounts of data are large, the data is sensitive, stored for long times and stored centrally. Privacy risks are significantly reduced when a system only determines the distances travelled, without monitoring the vehicle location for each moment or storing or processing these data.

Suppose a traffic monitoring system stores vehicle location data for a longer period of time in central databases and adds to that data from other databases: number plate registrations, criminal record registrations, passport registrations, etc. In such a large database, containing millions of files on persons or vehicles, each containing hundreds of attributes, the processing of data is only possible in automated ways. Using techniques such as data mining and risk profiling may be used to find patterns in an automated way, for instance, to investigate the origins of traffic jams or route preferences of drivers. Many of the applications described in the previous chapter are only possible with the use of pattern recognition in large amounts of data. Manual analysis of the data is usually unfeasible.

Automated pattern recognition may be used to map which vehicles were close to a crime scene at the moment the crime took place. Such a group of vehicles, limited, for instance, by a radius of five kilometers and two hours before and after the crime, may describe a risk group. People in this risk group may be investigated and interrogated. Among these people, there may be *false positives*, i.e., people who have nothing to do with the crime but just happened to be in the area at that time. This group may have to prove that they have nothing to do with the crime. Here the presumption of innocence is under pressure, since these people are considered to be guilty until proven innocent.

Limited reliability may also lead to limited effectiveness as a result of *false negatives*, i.e., the risk group does not contain the perpetrator(s) or other people the police wish to talk to. Obviously, it may be possible that the real perpetrator or potential witness was travelling by bike and hence was not registered in the system.

Apart from limited reliability of data and risk profiles, selection may also take place in undesired or unwanted ways. Once it becomes known that blue cars are more often of interest to the police, or car brand X is more often involved in accidents, this may result in prejudices and bias in looking for and approaching drivers. When these search preferences become

public, other parties may also use them for selection purposes. For instance, insurance companies may be interested in which vehicles are safe. With the use of such a criterion, the premiums may be adjusted or vehicles with high risks may be excluded from insurance. Risk profiles that become public knowledge may also have stigmatizing effects.[30]

For these reasons, it is often suggested that techniques like data mining should be prohibited. On the other hand, building very large databases which require automated processing and analysis of data offer interesting possibilities. And if data mining techniques improve the objections mentioned above might not exist anymore. Will it therefore be possible to avoid the matching and data mining of files by organisations?[31] Data mining may be questioned now, but might be used as common tool in the near future. A recent Dutch study describing the development of the use of technology used for investigation and security showed that use of technologies that were unthinkable ten to fifteen years ago are unquestionable now.[32]

5.2 Linking persons to vehicles

It is important to realize that all the traffic monitoring systems mentioned in chapter 2 are based on the identification of vehicles. However, many of the applications mentioned, in the end, also require identifying persons rather than vehicles. Charging for distances traveled, for instance, requires billing a person. This is usually done by linking a vehicle to a person, for instance, using the number plate registration database. This is based on the assumption that the person registered in this database is the owner of the vehicle or the person responsible for the vehicle.

It is possible to avoid being charged based on traffic monitoring by tampering with the link between vehicle and person. There may also be other reasons to avoid identification. For instance, using a stolen vehicle in a ram raid will provide leads about the victim of the car theft, but not necessarily about the perpetrator. By fixing a foreign number plate on a car and removing any OBUs, the location registration may be avoided. In these cases, someone is deliberately pretending to be someone else in order to obtain rights of the victim or avoid being caught. These are examples of *identity fraud*.[33] Road pricing based on traffic monitoring means that people are identified by means of their vehicle. By choosing another vehicle or ensuring the vehicle is no longer recognizable, the location registration will be undermined.

There are roughly three ways to deal with identity fraud.[34] The link between vehicle and person may be established more firmly with documentation, by posing questions and with biometrics. Documentation that can be used includes driving licenses and other documents that identify the driver, but also a vehicle registration certificate that proves that the driver is also the owner of the car. Questions can be asked when a driver is stopped, for instance by the

---

[30] J. Harvey, Stereotypes and Group Claims; Epistemological and Moral Issues, and Their Implications for Multi-Culturalism in Education, *Journal of Philosophy of Education*, Vol. 24, No. 1, 1990, pp. 39-50.
[31] Voor eeuwig te boek als een zatlap, Trouw, 19 November 2007 (<www.trouw.nl> search for *zatlap*>
[32] A. Vedder, et al., *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, The Hague: Rathenau Instituut/TILT, 2007.
[33] For more on definitions of ID fraud, see B.J. Koops and R. Leenes, ID theft, ID Fraud and/or ID-related Crime. Definitions Matter, *Datenschutz und Datensicherheit*, 30, 2006.
[34] J. van Kempen, *Catch Me If You Can! A study on Identity Fraud in the Netherlands*, Master's thesis, Eindhoven University of Technology, Eindhoven, The Netherlands, 2007.

police, or when billing takes place. Biometrics are not yet used in vehicle registration, but it is technologically conceivable that a car will only start if the legitimate driver identifies himself/herself with his or her fingerprint or by voice recognition.

5.3 Reliable or unreliable data: privacy is at stake

As indicated above, the reliability of the data available and the conclusions drawn from these data may be limited. The government may be careless with data sets, as was shown in a recent report of the Dutch Ministry of the Interior.[35] Basic data collections may be incorrect or incomplete. People who do not want to draw any attention may remove, change or sabotage OBUs. As a result, conclusions drawn from the data may not always be reliable, for instance, because vehicles and persons may be linked incorrectly. If a vehicle was at a particular location, this does not mean that the owner of the vehicle has also been at that location. The owner may then have to explain why the vehicle was at that location. This is a *privacy paradox*.[36] After all, the traffic monitoring system infringes the privacy by keeping track of the location of a vehicle, but to refute assumptions based on these location data, the data subject has to provide additional data about himself, which further infringes his privacy. It is not true that "innocent people have nothing to fear": if a person happens to be in the wrong place at the wrong time, he may become a suspect and will be treated as such.

Even if the reliability is reasonably good, location data may still lead to undesired or unwanted consequences from the perspectives of those involved. When it becomes known, for instance, that a vehicle is often parked at a particular address, this may reveal an extramarital affair. In many countries, speed cameras photograph the front of the car. Sometimes, these pictures are included with the speeding ticket that is sent to the speeder. The privacy of any person sitting next to the driver may be compromised. It may, for instance, reveal an affair. Vehicle location data may reveal this as well, even in cases where no speed limits are broken.

Location data in the hands of employers may offer the possibility to check whether an employee worked sufficient hours. Anyone driving more private kilometres than allowed may be traced, just like employees declaring expenses for more kilometres than were actually driven. Someone who overslept may claim he was in a traffic jam, but this may be checked.

In the hands of insurance companies, location data may also be used for other purposes. For instance, when particular car drivers often use routes where traffic accidents are common, the insurance company may decide to raise the premiums. Also the number of kilometres, the time and the type of car may cause differences in the premium, or, in case of unacceptable risks, exclusion from the insurance.

5.4 Conclusion

The use of traffic monitoring systems can lead to new information flows and storage of data related to the use of roads and the owner of a vehicle. The stored data can be used for data mining, risk profiling, and the linking of persons to a vehicle. However, reliability of the data available and the conclusions drawn from mining, profiling, and linking may be limited and

[35] Bosma, H. et al. (2007) *Data voor Daadkracht; gegevensbestanden voor veiligheid: observaties en analyse*, Report of the Safety of Information Streams Advisory Commission, April 2007.
[36] Custers, B.H.M. (2004) *The Power of Knowledge*, Tilburg: Wolf Legal Publishers.

as a result might have unwanted effects. To avoid these effects to occur traffic monitoring systems should process and store as little information as possible for the shortest possible period of time. For example, in the Stockholm Congestion Tax System (see the Swedish case study below) under normal circumstances data is deleted 28 days after payment and data of late payers is deleted 67 days after payment.

One could also think of introducing traffic monitoring systems which oblige road users to pay immediately. In that case the system only needs to *verify* the road use, but it is not necessary to *identify* the owner of the vehicle. In that case off course an anonymous payment system should be used. But what happens then when an anonymous immediate payment for whatever reason does not succeed?

6 Case Studies

In this chapter, seven case studies are presented, showing practices in Belgium (two cases), Germany (three cases), Sweden (one case), and The Netherlands (one case). The first Belgian case is based on video surveillance using ANPR, the second Belgian case is based on the presence of mobile phones in vehicles. The first German is on ANPR as well, whereas the second one is on a variant of on board equipment: the electronic license plate. The third German case is on car telematics. The Swedish case is on the Stockholm toll system which uses ANPR again. The Dutch case is on a system called *Kilometerprijs* which uses on board equipment in combination with satellites.

6.1 Belgium: Case 1 - Traffic monitoring via video surveillance

6.1.1 Introduction

In Belgium, traffic monitoring aims mainly to regulate traffic congestions around big cities and to control road offences, such as speed limits. As other European countries, fixed video cameras have been installed on the major road axes and police cars have been equipped with mobile cameras.

Two different kinds of video cameras should be distinguished: video cameras with no purpose of identification that control, e.g. traffic fluidity (regulation of the intervals of traffic lights, traffic diversion, etc.), and the ones with identification purposes usually devoted to road controls (radars).[37]

On the 20th of November 2007, the first radar equipped with a digital video camera was announced to be installed in Brussels to detect road offences.[38] Digital video cameras offer several advantages over analogical ones: the capacity of storage is higher, more lanes can be controlled, and it is possible to collect statistical data. The use of digital video cameras also allow to monitoring areas of difficult access such as tunnels, placing the video camera's data readers in a separate place more accessible to police (for the retrieval of data). The quality of images is similar to analogue video cameras. Digital zooming allows to identifying the car plate number and the type of vehicle.

These video cameras are expected to be connected to a control room via optic fiber in order to directly transmit and process the information. Meanwhile, the footing is recorded on a tape which can be taken off by police officers for further processing.

This chapter will focus on the legal constraint stemming from the use of fixed or mobile video cameras with identification purposes for the detection of road offences. Other projects, currently under development, will also be mentioned, namely, a urban toll system used on the motorways around Brussels, and two research projects funded by the Institute for Broadband Technology (IBBT), a Flemish research center, the first one (NextGenITS) tending to the

[37] Privacy Commission, Opinion of 34/1999 relative to images processing carried out via video surveillance systems, 13 December 1999, p.4.

[38] Gouvernement de la région Bruxelles-capitale, press realease, « Premier radar équippé d'une caméra digitale », 20 November 2007, <www.egsr.irisnet.be/site/20.11.2007.%20%20camera%20digitale%20FR.pdf>.

development of a new generation of intelligent transport systems for Belgium and the other VICATS (Video Content Analysis For Automated Traffic Surveillance) to the use of video cameras for the monitoring of trucks transporting dangerous goods in tunnels.

6.1.2 Legal constraints for traffic monitoring in Belgium

The Belgian Data Protection Authority (the Privacy Commission) has stated that control systems aimed at monitoring the fluidity of the road traffic should be placed at a distance which would preserve the anonymity of the "watched".[39] A video surveillance system should only allow the identification of the persons filmed when such identification appears strictly necessary to the achievement of the purpose foreseen. The collection of data for purposes of detection of road offences should thus be limited to the data strictly necessary for the identification of the offence and the offender. Data protection legislation poses a first limit to the information that can be processed. Additional legal constraints stem from specific road traffic legislation.

6.1.2.1 Application of data protection legislation: car number plates as personal data

Personal data means, according to the definition provided by article 2 of 95/46/EC Directive, any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person (Recital 26 of the Directive). It follows that 'as such, identification does not require knowledge of a person's name but it does require knowledge of some unique characteristics of the person relative to a set of other persons. What is of legal importance is the capability or potentiality of identification rather than the actual achievement of identification. Hence, data will not fail to be personal merely because the data controller refrains from linking them to a particular person.'[40]

In the commentary to article 2 of the amended Commission proposal, it was stated that "*a person may be identified indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.)".* This led the Data Protection Working Party to ascertain that "the terms of this statement clearly indicate that the extent to which certain identifiers are sufficient to achieve identification is something dependent on the context of the particular situation."[41]

---

[39] Privacy Commission, Opinion of 34/1999 relative to images processing carried out via video surveillance systems, 13 December 1999, p.4.
[40] L.A. Bygrave, Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002.
[41] Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007.

In that sense, this authority stated in its opinion on video surveillance that "image and sound data that relate to identified or identifiable natural persons is personal data even if they do not concern individuals whose faces have been filmed, though they contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers".[42]

It follows that whenever the car number plate can be linked to the owner of the car, the data will qualify as personal.

With regard to attribution of car number plates, two systems are generally used in Europe: either the number identifies a specific car, e.g. in France, or it is personal and directly identifies the owner. In Belgium, the plate is attributed to a person and not to a vehicle. The ownership of the plate remains within the Public administration (in Belgium within the Federal General Directorate for Mobility and Road Safety) who owns the "vehicle's directory".

Traffic monitoring which implies the scanning of car number plates in Belgium will thus fall under the scope of data protection laws.

6.1.2.2 Limitation to the process of identification of the offender

Databases against which the image is checked

For purposes of road offences processing the car number plate is checked against two different databases: the vehicle's directory for the identification of Belgian car number plates and the Schengen Information System (SIS)[43] for European ones.

The directory contains information with regard to the owner of the car license plate, such as name, address and national number if he/she has the Belgian nationality (article 8 of the Royal Decree of 20 July 2001[44]).

This information could only be used for limited purposes listed by the Royal Decree of 20 July 2001 (Article 6§2), such as the investigation and pursuit of criminal offences, for the needs of administrative police or road police.

In order to enhance the traceability of vehicles, a legislative proposal is intending to reform the current "vehicles' directory" and to create an "authentic source of data relative to vehicles". The concept of "authentic source" is a core concept of e-governement in Belgium. It means that it becomes possible for significant data (national number, VAT (Value Added Tax) number, etc.) to identify a unique public authority in charge of managing the databases related to this specific data, i.e. the storage and actualization of the data it contains. Whenever

[42] Data Protection Working Party, Opinion on the Processing of Personal Data by means of Video Surveillance, WP89, 10 February 2004.
[43] The Schengen area and cooperation, Europa.eu <europa.eu/scadplus/leg/en/lvb/l33020.htm>.
[44] Royal Decree on vehicles licences, 20 July 2001, *M.B.* 8 August 2001.

a public authority needs the data, it can direct its request to the "authentic source" instead of creating a new database. This is meant to reduce incoherence and redundancies.[45]

This source is foreseen to be used for a number of public tasks and will also provide legal basis for the reselling of the data to the private sector. In its Opinion on the creation of an authentic source of vehicles[46], the Privacy Commission however deplored that the concept of "public tasks" was not defined well enough and remains vague. The data protection principle of finality[47] mandates data to be collected for specified, explicit and legitimate purposes. The Privacy Commission recalls to that effect that the obligation to clearly define by law the purposes of the authentic sources stems from the principle of legality (article 22 of Belgian Constitution) and from the requirement of *foreseeability* of the norm as contained within article 8 European Convention on Human Rights (ECHR). This obligation relates to the legal objectives of the source but also to the limits within which the source can be used.

According to the official information available, the authentic source of vehicles' data mainly aims at fighting against car frauds and hijacking.[48]

The car number plate could also be checked against the Schengen Information System (SIS) for stolen or hijacked cars. This database only contains information relative to the more serious cases: data can only be introduced by judicial mandate.

Identification of the offender

When the offender has not been identified during the observation of the offence, article 9 of Law 4th August 1996[49] modifying articles 67bis and ter of the Law on Road Traffic of 1990 stipulates that the offence is reputed to be committed by the owner of the car license plate.

Additional rules govern the cases where the car license plate is owned by a legal person or when the owner has changed. In the first case, the article obliges, in a delay of 15 days, the representatives to communicate the identity of the driver or, if it is unknown, of the person responsible for the vehicle.

In the latter case, if the identity of the driver has changed, the current driver has to communicate the identity of the previous driver in the moment of the commission of the offence.

---

[45] Wall-on-line : l'e-gouvernement wallon, Accès aux sources de données, <egov.wallonie.be/pa0403.htm>.
[46] Privacy Commission, Opinion 42/2006 on the law proposal creating an authentic source of vehicles' data, of 18 October 2006.
[47] Under the finality principle, data controllers must obtain data only for specified and legitimate purposes, and must not carry out any further processing which is incompatible with those purposes. For more information about data protection principles, see FIDIS, D.11.1. "Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity", available on-line at: <www.fidis.net/resources/deliverables/mobility-and-identity/int-d111000/doc/4/>.
[48] Ministers' Council, Press release of the Ministrers' Council of 23 June 2006, Traçabilité des véhicules, available online at: <www.residencepalace.be/archive/20060623/868e03129a5b88379c6feac0de5168ae/?lang=fr>.
[49] Law of 4th August 1996 relative to the autorisation and use in road traffic of automatic devices in presence or absence of official agent, *M.B.* 12 September 1996

6.1.2.3 Data protection safeguards

The general principles are contained in the Belgian Data Protection Act of 1992. A specific act has been adopted in 1996 in order to regulate the use of automatic devices in the field of traffic monitoring which contains some provisions with regard to the observation of traffic offences.

The provisions of the Data Protection Act have been further specified in the Video Surveillance Act of 21 July 2007[50] for processing data arising from video surveillance with security purposes. However, this act expressly excludes from its scope of application the processing covered by act of 4 August 1996 and thus will not be taken into account in this analysis.

The processing of car number plates is limited in several ways in order to safeguard drivers' privacy. First of all, a strict respect of the finality principle is ensured. The processing can only be carried out by police forces, the public authority in charge of monitoring traffic offences. The use of car number plates' data is strictly limited to the purposes foreseen by law. In that sense, the Privacy Commission denied to bailiffs the access to the vehicles' directory to identify fraudsters in private parking.[51] The Privacy Commission considers that article 6 of the Royal Decree of 20th July 2001 strictly defines the purposes for which the directory could be used and such processing did not fit in any of the cases listed. The ground relative to the payment of taxes due for the use of the vehicle could not permit such processing. Moreover, the highly intrusive character of such access is considered disproportionate as other means less intrusive could be used to prevent illegal parking, such as the installation of barriers at the exit of the parking.

Also the re-use of images taken is strictly limited to judicial purposes relative to the repression of traffic offences committed on public roads and for the need of traffic monitoring. (Article 8 of the Act of 4th August 1996 modifying article 62 of the Law on road traffic of 18 July 1990).

The legality principle is also ensured in so far as the processing is based on the need for the performance of a public competence and thus limited to the public authority in charge of road offences, i.e. the police.

Finally, information should be provided to data subjects in an appropriate, clear and detailed way, in order to ensure that the data subjects are aware of the fact that they are being filmed. The information should contain the name and address of the controller or of his representative, the finality of the processing, the existence of an access and modification right, as well as the recipients of these data. This is usually done by placing an information notice in the public area close to the video camera.

6.1.3 Urban toll in Brussels[52]

The installation of an urban toll system around Brussels has been recently raised. The toll is expected to reduce road traffic and all negative impacts it could have on Brussels inhabitants

[50] Law of 21 March 2007, regulating the installation and use of video cameras, *M.B.* 31 May 2007
[51] Privacy Commission, Opinion 37/2003 of 28 August 2003.
[52] Based on the information contained in Bruxelles et le péage urbain : une solution proposée pour 2015 : <www.ieb.be/article/843/>.

(pollution, noise pollution, etc.). Even if the idea has been temporarily put aside because of the fear of part of the politicians to have companies migrating outside Brussels, causing huge economical losses for the region, there is still significant political support towards the idea[53].

Several possibilities are envisaged, one being to install a toll based on automatic number plate recognition (ANPR), as the one in London, another being to use dedicated short range communication (DSRC), or finally a mixed solution. The different studies carried out so far suggest a model based on differentiated pricing depending on hours and an electronic toll as the one used in London.

The system based on ANPR relies on the use of automatic recognition software in intelligent video cameras. These cameras would lead to create three new databases:

- a database with car number plates read during the day
- a database with number plates of cars having paid the tax
- a database which compares the information contained in the aforementioned ones aiming at identifying fraudsters. To that effect, the information is checked against the vehicles' directory.

The use of APNR, despite implying the processing of location data, appears to be less intrusive than others based on the DSRC technology in so far it only registers data relative to the passage of the car at the entrance and exit of the restricted area. With an APNR system, the car plate number is only read when the car enters and exits the restricted area, whereas the DSCR technology permits to carry out a complete follow-up of the itinerary of the car within the restricted area (and adjust the amount of the tax to be paid to the distance driven). However, preference seems to go towards a DSCR system on the basis of future development of Galileo and road safety systems tending to install GPS[54] in all cars; or on a system based on the combination of APNR and DSRC.

The processing of location data should be in any case consistent with the existing legislation, especially with the Act of 4th August 1996 and the Data Protection Act. Specific attention should be paid to the risks arising from the significant amount of location data in case the toll would be managed by private parties due to the increased possibilities of individuals' tracking.

6.1.4 Other projects of interest

Two other projects led by the IBBT, a Flemish research center, can make traffic monitoring to evolve substantially in Belgium. A brief highlight of both projects' objectives is given in this section, based on the information publicly available at the moment of writing. It intends to provide an overview of the trends followed in this country.

NextGenITS

[53] Pas de péage aux portes de Bruxelles... pour le moment , Le VIF.be, 04/01/2008 <www.levif.be/actualite/belgique/72-56-11231/pas-de-peage-aux-portes-de-bruxelles----pour-le-moment.html>.
[54] Global Positioning System, Wikipedia <en.wikipedia.org/wiki/Global_Positioning_System>.

The *Next Generation of Intelligent Transport System* (NextGenITS) project gathers some of the most prominent players in the Belgian ICT sector to cooperate with research institutes and governments to develop and demonstrate a number of ITS services. The following services will be demonstrated: e-call, traffic information, intelligent speed adaptation, road charging and cooperative vehicle systems. These services which either or both have a big social and commercial potential will be demonstrated as a preparation for market introduction through public-private partnerships.

The different applications will be based on European standards to ensure interoperability between different market players and across geographical borders. Furthermore, specific research will be done related to the integration of the different applications on a generic multi-application platform.

The project collaborates with other regional and national initiatives within the framework of a European FP7 project proposal. Besides being a tool to accelerate the introduction of next-generation ITS services to ensure sustainable mobility in Flanders and to reach ambitious safety and environmental targets, this project also will work as an enabler preparing the industry for the European and global ITS market which is generally expected to grow exponentially between 2010 and 2015.

VICATS
VICATS stands for Video Content Analysis for Tunnel Surveillance, and focuses on the detection and tracking of trucks carrying dangerous goods in tunnels. It has been observed that most tunnel fires are caused by trucks of which the mechanical brakes are blocked and catch fire due to the heat. Consequences can be devastating. This project, which has been recently launched (June 2008) intends to provide solutions for the prevention of accidents in tunnels in response of the accidents of the recent years.

6.1.5 Conclusion

Video surveillance with identification purposes is mainly used in Belgium for the detection of traffic offenses. The data protection issues have been dealt with by specific legislation which has defined, amongst other, the competent authority authorised to access the vehicle directory and the cases where the data could be re-used or transferred to third parties.

Video surveillance is now planned to be used for other purposes such as the implementation of an urban toll, in combination with other technologies, or for road safety (VICATS). This raises specific problems in terms of data protection, mainly related to the creation of new databases, and in particular in relation with the use of the vehicles' directory. These problems will have to be dealt with either by the specific legislation that will regulate these new uses or by an interpretation of the general data protection principle set up by the Data Protection Act. The opinion on the new vehicles' directory issued by the Belgian Privacy Commission revealed however some important flaws from a privacy perspective, in particular with regard to the vague terms used to regulate the purpose of the directory.

6.2 Belgium: Case 2 - Floating car data[55]

6.2.1 Introduction

The Ministry of the Flemish Community (Ministerie van de Vlaamse Gemeenschap) initiated in September 2004 along with the Belgian mobile telephone operator Proximus and the UK-based company ITIS Holdings plc, which is specialized in traffic information, a project on Floating Car Data in Flanders[56]. Floating Car Data (FCD) [57] is a method to determine the traffic speed on the road network, which can be realised through the use of several technologies, like CDMA[58], GSM[59], UMTS[60] and GPRS.

The project was conducted in the region of Antwerp, due to the extensive road works that were taking place at the Ring of the city at that time. During the validation phase of the project, which ended in January 2006, it was examined whether the collection of anonymous traffic and location data through the monitoring of the mobile phones that are inside a vehicle could give accurate traffic information and estimation times[61]. This technology can be very useful in places where there are no detection loops or cameras, for instance.

The floating vehicle technology (Estimotion)[62] developed by ITIS Holdings plc was used for the actual gathering of the data that were further analysed by the Traffic Centre of Flanders (Verkeerscentrum Vlaanderen) for their accuracy and their added value to traffic management. The technology used anonymous data of active mobile phones in vehicles. Although during the project no information about the origin and the destination of the vehicles was derived from the traffic data, such information could be obtained after modifying the software, according to ITIS Holdings plc.

The actual results of the project showed that when the traffic flow was free, the prediction was mostly accurate, while in congested conditions the absolute values for the predicted travel times were not accurate, but rather optimistic. However it is to be mentioned that in general the technology was able to detect in a quite accurate way the traffic rends over time per road segment[63]. The data collected during this project were kept in a database and were used for traffic analysis.

---

[55] Description extracted from the Deliverable 11.5, Report on Belgium.
[56] Not much information about the project is available to the public according to the internal agreement of the relevant parties.
[57] Floating Car Data, Wikipedia <en.wikipedia.org/wiki/Floating_Car_Data>.
[58] Code division multiple access, Wikipedia <en.wikipedia.org/wiki/CDMA>.
[59] Global System for Mobile communications, Wikipedia <en.wikipedia.org/wiki/GSM>.
[60] Universal Mobile Telecommunications System, Wikipedia <en.wikipedia.org/wiki/UMTS>.
[61] Press release of the Ministry of the Flemish Community on 11 January 2006, available online at <www.mobielvlaanderen.be/persberichten/artikel.php?id=115>.
[62] Press release of the Ministry of the Flemish Community on 02 September 2004, available online at <www.agoria.be/ICT-TIC-Flash/nl/87/87-10%20pers%20vl%20gem%5B1%5D.doc>.
[63] See note 50.

6.2.2 Analysis of the case study

According to a press release of the Ministry of the Flemish Community one of the objectives of the Floating Car Data in Flanders project was to examine whether the collection of anonymous traffic and location data through the monitoring of the mobile phones that are inside a vehicle could give accurate traffic information and estimation times[64]. It seems thus that initial goal of the project was to collect and process *anonymous* traffic and location data for the needs of the project. However, it was revealed that information about the origin and the destination of the vehicles could be obtained from the traffic data, after a modification to the software used for the project. It shall be reminded that very few detailed information about the project is available to the public and therefore our analysis will be theoretical when it comes to specific details.

A main point of our analysis is whether the traffic and location data collected and processed in the project are anonymous or personal data. Although no personal information was derived during the project, the fact that the data –in an apparently easy way of modifying the software- can be linked to a vehicle and subsequently to a driver and a mobile user renders them personal data. Recital 26 of the Data Protection Directive reads that in deciding whether data could be used to identify a particular person "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". The broad conception of the notion of personal data means that data is usually presumed to be 'personal', unless it can be clearly shown that it would be impossible to tie the data to an identifiable person (that is, unless the data is truly anonymous)[65]. Therefore in the Floating Cara Data project the traffic and location data that are collected via a mobile phone, which can in most of the cases be easily linked to a natural person, shall be treated as personal data. As a result the processing of the traffic and location data shall take place according to the provisions of the data protection directive, as transposed into the Belgian legislation via the Belgian Privacy Act (BPA).

Within the project it is important to define three major categories of parties. The data subject, the data controller and the data processor. The 'data subject'[66] shall be considered any natural person which is the subject of the personal data, i.e. the user of the mobile phone and in most cases the driver of the car (for detailed analysis of this point we would need more information on the project, which is not available). The 'data controller' is "the natural or legal person, the factual association or public authority that alone or jointly with others determines the purposes and means of the processing of personal data"[67], while the processor is defined in Article 1§5 BPA as "any natural person, legal person, factual association or public authority that processes personal data on behalf of the controller, except for the persons who, under the direct authority of the controller or the processor, are authorised to process the data". With regard to the differentiation between data controller and data processor as a rule of thumb it can be said that the data controller is liable for violations of the data protection legislation, while the role of the data processor is limited[68].

---

[64] See note 50.
[65] C. Kuner, *European Data Privacy Law and Online Business*, Oxford University Press, 2003., p.51.
[66] Art. 1§1 BPA.
[67] Art. 1§4 BPA.
[68] Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, 2003, p.62

It is important to note that mere storage of personal data by the mobile operator constitutes 'data processing', so that simply storing data on a server or other medium is deemed to be processing, even if nothing else is being done with the data. The use of location and traffic data for the scope of this project shall be based on a legal ground, as described in article 5 BPA, such as the consent of the user or the public interest. The fact that the Ministry of the Flemish Community is also involved in the project could justify the necessity of processing of the data for the public interest. In this case the processing of the data could be based on art. 5(e) of the BPA claiming the fulfilment of a task of public interest (openbaar belang).

In any case, according to the finality (or else purpose limitation) principle, the purpose for which the personal data are processed shall be clearly defined. In the Floating Car Data project, the data are processed in order to derive traffic information, traffic data and to enhance estimation times. This means that the data can not be collected and used for other purposes, either by the mobile operator or by the other project partners. However the further processing of data[69] is allowed without other reasoning if the data are further processed in a way compatible with the initial specified, explicit and legitimate purposes, taking into account all relevant factors, in particular the reasonable expectations of the data subject and the applicable legal and regulatory provisions.

According to the BPA the data shall be processed in a fair and lawful way[70]. Essential for this is that the relevant data subject, at the time of the obtaining, or very soon afterwards, is provided with certain information, mainly information mentioned in article 9 of the Belgian privacy act.[71] Given the nature of the project this could be done by placing clear notification signs in the areas where the collection of data is taking place. Furthermore, only data that are "adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed"[72] shall be used in the project. Their accuracy shall be guaranteed throughout the life of the project and they shall be deleted or fully anonymised when the specified purpose for which they were collected has been achieved.

The Commission for the protection of privacy about the processing shall also be notified of the processing of the data, according to the procedure set out in art. 17 of the BPA.

The Floating Car Data project entails the collection of traffic and location data by a mobile operator and therefore the definitions of art. 2 nr. 3 (electronic communications networks) and nr. 5 (electronic communications services) of the Electronic Communications Act (ECA) shall be taken into consideration. The fact that no specific information about the kind of traffic and location data that is used in the project is available, does not allow us to go into an in depth analysis of the details of their processing, according to the specific provisions of the Electronic Communications Act. Nevertheless the following general remarks need to be made.

According to art. 1 nr. 6 ECA traffic data means "any data processed for purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". Such data must be erased or made anonymous when it is no longer needed for the

[69] Article 4§1 Nr. 2 BPA.
[70] Article 4§1 Nr. 1 BPA.
[71] Carey, P., *E-Privacy and Online Data Protection*, Butterworths, 2002, p. 54.
[72] Article 4§1 Nr. 3 BPA.

purpose of the transmission of a communication. For the sole purpose of billing and interconnection payments specific data, mentioned in art. 122§2 act on electronic communications may be processed until the end of the period during which the bill may lawfully be challenged or payment pursued. Further exceptions are foreseen with regard to the retention of data for law enforcement purposes, as it will be elaborated below.

Location data[73] means "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of an end-user of a publicly available electronic communications service". Article 2 nr. 9 of the ECA defines the term 'service with location data' as 'a service which requires a special use of location data that goes beyond what is absolutely necessary for the transmission or the billing of a communication').

According to Belgian legislation[74] the provider of electronic communications services or networks (including resellers) shall retain the 'traffic data' and 'identification data' of end-users for a period between 12 and 36 months. However, the Belgian legislation is not, as yet, enforceable as the necessary royal decree that will regulate some more specific issues relating with the retention of data is still not adopted. The decree will need to define the exact retention period and under what conditions the providers will register and retain the aforementioned data. This will be done for the investigation and prosecution of criminal acts, for the tracking of malicious calls to emergency services and to enable the research of the Ombudsman for Telecommunications in revealing the identity of people making improper use of electronic communications services or networks.

As a concluding remark it shall be noted that the Council of Ministers (Ministerraad) adopted a preliminary draft concerning the creation of an authentic source for vehicle data, via the creation of a database (see also the Belgian case on video-surveillance). Although the creation of such a database is seen as valuable tool in the fight against vehicle criminality and in the frame of data exchange within the Schengen and Eucaris Agreements, it is definitely not free of data protection and privacy concerns. The Belgian Privacy Commission has already published an Opinion on the topic[75], which has drafted relevant guidelines.[76]

[73] Art. 2 Nr. 7 act on electronic communications
[74] Article 126 of the act on electronic communications. This Article is currently under revision but no official amendment has been accepted at the time of the writing of this deliverable.
[75] ADVIES Nr 42 / 2006 van 18 oktober 2006, "Advies betreffende het voorontwerp van wet houdende de oprichting van een authentieke bron van voertuiggegevens", available online at <www.privacycommission.be/nl/docs/Commission/2006/advies_42_2006.pdf >.
[76] Privacy Commission, Opinion 42/2006 on the law proposal creating an authentic source of vehicles' data, of 18 October 2006.

6.3 Germany: Case 1 - Automatic Number Plate Recognition (ANPR)

6.3.1 Technical Background[77]

Technically automatic number plate recognition uses basic technologies already available for years. Typically the following steps are used:

1. Taking a digital image
2. Locating the number plate of the car on the image
3. Optimisation of the image of the number plate
4. Converting the numbers on the plate into ASCII data using Optical Character Recognition (OCR)
5. Comparing the digitised numbers of the plate against a reference database
6. Verifying of potential hits reported by the system
7. Taking appropriate action depending of the characteristics of the hit

Figure 6.1 shows the steps introduced:

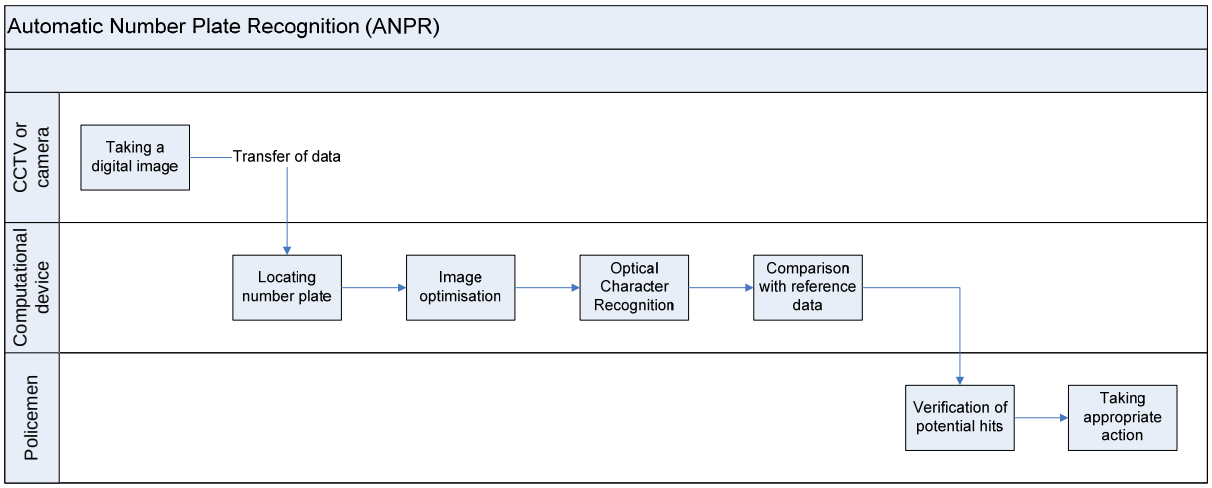

Figure 6.1: Steps of Automatic Number Plate Recognition (ANPR)

Digital image as starting point for number plate recognition are typically taken from two types of sources. While in the U.K. the pictures are taken from CCTV[78], in Germany in addition cameras are used that take a digital image. For this purpose cameras are used that are similar to speed cameras or cameras used to control traffic for toll collection purposes[79]. These cameras can be used in a mobile way as they are installed in cars[81] or permanently mounted

[77] All URLs used as reference in this sub-chapter were checked on 19th of December 2007.
[78] Closed-circuit television, Wikipedia <en.wikipedia.org/wiki/Closed-circuit_television>.
[79] For example the PoliScan-system produced by VITRONIC (see <www.vitronic.de/verkehr/>) .

e.g. on bridges used for toll collection systems or traffic signs.[80] A hidden installation also is technically[81] and legally[85] possible.

The digital picture is transferred to a computer where the further steps are carried out. For this purpose typically a special application is used.[82]

In the second step the number plate is been located and distinguished from other writings on the car, e.g. advertisements. Obviously some systems report a potential hit if no number plate can be found.[83]

In the third step the image of the isolated number plate is optimised. This mainly includes the following steps[78]:

- Correction of the plate orientation,
- adjustment of the plate sizing and
- optimisation of brightness and contrast of the image of the number plate.

In the fourth step Optical Character recognition (OCR) is used to transfer the digital image into ASCII-code (ASCII stands for American Standard Code for Information Interchange, a digital representation of letters, numbers etc. through a 7 bit digital code[84]).

In the fifth step the converted number plate data is checked against a reference database. In Germany typically two databases are used: a national database called INPOL, which lists amongst others, objects that are searched for by the police also number plates, and the Schengen Information System (SIS).[85] While in the national German INPOL system currently 500,000 number plates are stored, the SIS stores 2,000,000 number plates Europe wide.[86] In some cases partial information of number plates is stored in these databases only.[85]

In this context it is important to take a look on reasons why a number plate may be stored in one of these reference databases, as they can differ widely. Typically known examples are:

- The holder reports that the number plate got lost or was stolen
- The car was stolen
- Permit to operate the car became invalid as car tax or insurance rates were not paid
- The car has been used to commit a crime e.g. a robbery, stealing of gasoline at gas stations etc. and the number plate was (fully or partially) recognised
- The holder is searched for various reasons

In case a corresponding full or partial entry is found in the reference databases a hit is displayed by the application carrying out the number plate data processing.

---

[80] The Federal Land of Hesse operates a static ANPR at the "Elzer Berg" on the motorway A3, see <www.uni-potsdam.de/db/elogo/ifgcc/index.php?option=com_content&task=view&id=6648&Itemid=128&lang=en_GB>.
[81] See <www.vitronic.de/verkehr/poliscansupstrongemsurveillanceemstrongsup-poliscansupstrongemsmartemstrongsup/>.
[82] See e.g. PoliScan classic manufactured by the VITRONIC GmbH, <www.vitronic.de/verkehr/poliscansupstrongemofficeemstrongsup/>.
[83] This can be concluded from <www.autosieger.de/article10692.html>, where the fact is reported that 20% of the hits achieved in the Federal Land of Bavaria from January to October 2006 referred to cases where the number plate got lost or was stolen.
[84] See <de.wikipedia.org/wiki/ASCII>.
[85] See <https://www.datenschutzzentrum.de/polizei/060426-kfz.htm>.
[86] See <www.welt.de/welt_print/article1383896/Massenkontrolle_von_Autos_auf_dem_Pruefstand.html>.

In the sixth step this potential hit is verified, as there are a number of well known reasons for technical failure of the system. Known technical problems are among others:[78]

- Poor image quality due to low resolution (e.g. the car was too far away), blurry picture (motion blur due to high speed or bad light conditions) or low contrast (e.g. caused by reflections, poor lighting, dirt etc.)
- An object is obscuring the plate or parts of it
- The character recognition fails or leads to wrong results due to the fact that foreign plates unknown to the system were scanned. Number plates show a large variety in fonts and types of numbers, depending on the issuing country and the age of the number plate
- The plate was obscured deliberately using covering, dirt or special sprays or foil.

In Germany, up to 40% of hits checked in this step seem to be wrong.[87]

In case a hit has been confirmed, an appropriate action is taken, based upon context data stored in the reference databases. Typical possible actions include:[85]

- In the context of an ongoing observation the hit may be stored in the police databases together with date, time and location. This data may be used at a later time.
- A proceeding may be initiated by the police, resulting in a fine, trial or the like.
- In case of emergency immediate action may be taken by the police to stop the car and to search it, or to arrest the driver or other persons in the car.

6.3.2 Effectiveness of Number Plate Recognition

The effectiveness of number plate scanning in Germany is disputed. So far little data with respect to effectiveness became publicly available.

The Federal Land of Bavaria carried out a test for number plate scanning in 2002/2003 for six months.[88] In the testing 282 hits were confirmed, leading to 114 cases in which holders or cars were searched for. In this context four very expensive cars could be secured. In 168 cases the number plate was searched for because it was stolen or became invalid due to not paid tax or insurance rates.

Additional data from the Federal Land of Bavaria became available for January to October 2006.[89] During this period of time 45 Mio number plates were scanned. In 0.03% of scanned number plates a confirmed hit was generated (round about 13,500 cases). 40% (round about 5,400) of these hits referred to insurance rates that were not paid, additional 20% (round about 2,700) referred to lost or stolen number plates.

From March 2007 to November 2007 in the Federal Land of Hessen 1 Mio number plates were scanned, resulting in 300 confirmed hits. Among these hits two third referred to missing insurance (in most cases due to not paid insurance rates), in one case burglars could be arrested.[90]

An evaluation of the effectiveness and technical use of mobile and fixed ANPR systems is currently being carried out in the federal Land of Schleswig-Holstein. The trial phase started

[87] See <www.datenschutzverein.de/Pressemitteilungen/PE-Kfz-Abgleich-20071119.pdf>.
[88] See <www.stmi.bayern.de/presse/archiv/2004/80.php>.
[89] See <www.autosieger.de/article10692.html>.
[90] See <www.focus.de/magazin/kurzfassungen/focus-_aid_139572.html>.

in August 2007 and will last until July 2008[91] and will involve testing of one mobile and one fixed system. During this trial phase only search data aiming at safeguarding property rights of cars will be used for matching with the search database INPOL.

6.3.3 Legal basis for ANPR in Germany

It is possible to differentiate between three main objectives of police tasks. Law enforcement authorities are responsible for investigations following an individual's punishable action (repressive – law enforcement[92]). A second long-established task of police forces is the prevention of crime and punishable actions (preventive measures taken to avert an imminent threat[93]). Traditionally, police laws of the German states linked police powers regulated in these laws to the existence of an "imminent threat to a legally protected interest". In the past 20 years the temporal link of police powers has been significantly shifted and preventive powers today comprise so called *Vorfeldmaßnahmen* (preventive measures prior to an imminent or concrete threat).

Generally, if a fundamental right laid down in the German constitution (*Grundgesetz* – Basic Law) or derived by the German constitutional court based on these codified fundamental rights is restricted, a specific law complying with the principle of certainty must be passed or already exist, allowing this restriction. This principle is called *Gesetzesvorbehalt* - provision of legality. Limitation of a fundamental right is permissible only if a predominant public interest is protected.

The rights and obligations of the German police are regulated in the police laws of the German states as well as the federal *Strafprozeßordnung* – Code of Criminal Procedure.[94]

According to the principle of concurrent legislative powers, regulated in Articles 72 and 74 of the Basic Law, the constituent German states hold the legislative power as long as the federation does not decide to regulate a specific branch of law conclusively. If a conclusive federal law exists, the German states may not pass additional or even contradicting provisions in this branch of law. The federal Code of Criminal Procedure regulates law enforcement measures conclusively.[95] No federal regulation permitting ANPR is in place. Thus, the provisions existing in some of the German states must not aim at law enforcement but only at prevention of crime. One main purpose of ANPR is to detect stolen cars, to protect car owners property rights in case his car got stolen and to enable an investigation of the theft. These aims are predominantly part of law enforcement and some authors consequently doubt that German states have the power to legislate ANPR in their state police laws.[96] Furthermore, ANPR is used to detect cars without permit to operate the car in case the car tax or insurance rates were not paid.

---

[91] See <www.daten-speicherung.de/data/Landespolizeiamt-SH_Verfuegung_2007-08-14.pdf>.
[92] The German term for law enforcement is *Strafverfolgung*.
[93] Called *Gefahrenabwehr* in German.
[94] A comprehensive presentation of German police law can be found at H. Lisken and E. Denninger (2007): „Handbuch des Polizeirechts". For a description of general police tasks see p. 303 et seq.
[95] H. Lisken and E. Denninger, Handbuch des Polizeirechts, 2007, p. 369.
[96] See C. Arzt, Video- und Mautkontrollen – Autofahrer unter Generalverdacht, 2006. Available at <www.adac.de/images/Arzt-FHfV-ADAC-FG-Gl%E4serner-Autofahrer-Referat-28Sept06_tcm8-166157.pdf>.

Currently, ten[97] of the 16 German states have regulated a provision allowing automatic number plate recognition in their state police laws. Further provisions permit police measures which can also include determining the location of an individual. These police powers include observation, monitoring, dragnet controls, localisation of a suspect's cell-phone, and optical surveillance.

The following table presents an overview of the ten existing provisions permitting automatic number plate scanning:

State	Provision	Effective from	Constitutional Complaint
Bavaria	Article 33 Section 2 (2, 3), Article 38 Section 3, and Article 46 Section 2 PAG[98]	1.1.2006	no
Bremen	Article 29 Section 6 BremPolG[99]	28.2.2006	no
Brandenburg	Article 36a BbgPolG[100]	18.12.2006	no
Hamburg	Article 8 Section 6 HmbDVPolG[101]	16.6.2005	no
Hesse	Article 14 Section 5 HSOG[102]	22.12.2004	yes
Mecklenburg-Western Pomerania	Article 43a SOG MV[103]	10.7.2006	no
Lower-Saxony	Article 32 Section 5 Nds. SOG[104]	14.12.2007	no
Rhineland-Palatinate	Article 27 Section 5 POG[105]	2.3.2004	no
Saarland	Article 27 Section 3 SPolG[106]	12.9.2007	no
Schleswig-	Article 184 Section 5 and 6	13.4.2007	yes

[97] These ten states are Bavaria, Bremen, Brandenburg, Hamburg, Hessen, Lower Saxony, Mecklenburg-Western Pomerania, Rhineland-Palatinate, Saarland, and Schleswig-Holstein.
[98] Polizeiaufgabengesetz. Available at <by.juris.de/by/gesamt/PolAufgG_BY_1990.htm>.
[99] Bremisches Polizeigesetz. Available at <www.umwelt-online.de/regelwerk/allgemei/laender/hb/polg1.htm#p29>.
[100] Brandenburgisches Polizeigesetz. Available at <www.landesrecht.brandenburg.de/sixcms/detail.php?gsid=land_bb_bravors_01.c.14184.de#36a>.
[101] Gesetz über die Datenverarbeitung der Polizei Hamburg. Available at <hh.juris.de/hh/PolDVG_HA_P8.htm>.
[102] Hessisches Gesetz über die öffentliche Sicherheit und Ordnung. Available at <www.hessenrecht.hessen.de/gesetze/31_oeffentliche_sicherheit/310-63-hsog/paragraphen/para14.htm>.
[103] Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern. Available at <mv.juris.de/mv/SOG_MV_P43a.htm>.
[104] Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung. Available at <www.lexsoft.de/cgi-bin/lexsoft/niedersachsen_recht.cgi?chosenIndex=Dummy_nv_6&xid=173060,33>.
[105] Polizei- und Ordnungsbehördengesetz. Available at <rlp.juris.de/rlp/PolG_RP_P27.htm>.
[106] Saarländisches Polizeigesetz. Available at <www.saarland.de/dokumente/thema_justiz/2012-1.pdf>.

Holstein	LVwG[107]		

At least one other state is preparing provisions permitting ANPR, the state of Baden-Wuerttemberg.[108]

6.3.4 Privacy implications

Automatic number plate recognition involves five steps of data processing:

- data collection: via an optical sensor (digital camera),
- data processing: converting the numbers on the plate into ASCII,
- data storage: the ASCII data is stored,
- data use: the data is transmitted to a central database,
- data use: the digitised numbers of the plate are compared against the reference database.

Automatic number plate recognition is privacy relevant. The national car register[109] is run by the Federal Office for Motor Traffic (*Kraftfahrtbundesamt*). The register contains the following data[110]:

- number plate,
- attributes of the car,
- ownership of the car,
- third party insurance,
- name and surname of the car owner,
- day and place of her birth,
- sex,
- address.

The collection of the number plate thus allows identification of the car owner. Usually a car is driven by its owner. In this case the number plate is a direct identifier as it allows establishing a connection between the vehicle and the owner. However, if the car is used by another person, the owner will in almost every case be able to identify the car's driver at a specific point in time. In this case the driver of the car is "identifiable"[111]. In addition during ANPR information is collected regarding the fact that a car with that particular number plate drove in a specific direction at a specific point in time. Furthermore, the location of the mobile or fixed ANPR system is recorded, too, and hence the location of the car.[112]

---

[107] Landesverwaltungsgesetz. Available at <sh.juris.de/sh/gesamt/VwG_SH.htm#VwG_SH_P184>.
[108] See Heise Online: "Baden-Württemberg will Befugnisse der Polizei ausweiten", 22.8.2007. Available at <www.heise.de/newsticker/meldung/94747>.
[109] *Zentrales Fahrzeugregister (ZFZR).*
[110] Regulated in Article 33 *Straßenverkehrsgesetz.* Available at <www.gesetze-im-internet.de/stvg/BJNR004370909.html>.
[111] See Article 29 Data Protection Working Party: „Opinion 4/2007 on the concept of personal data", page 12 et seq.
[112] See decree on the test of APNR systems in Schleswig-Holstein. Available at <www.daten-speicherung.de/data/Landespolizeiamt-SH_Verfuegung_2007-08-14.pdf>.

The German Constitutional Court ruled that already the collection of data is a restriction of the right of informational self-determination if this data collection then makes available the data for further analysis and matching with a reference data base.[113] Even though this decision was established with regards to eavesdropping of telecommunication, the court may apply the general rational behind it also in this case.

6.3.5 Legal concerns

The German Constitutional Court has in a number of rulings laid down thresholds for police powers and their impact on privacy (in Germany: the constitutional right of informational self-determination) and other fundamental rights.

According to these principles, a limitation of fundamental rights must be proportionate, whereby the proportionality principle in German constitutional law means that

- the interference must aim at achieving a legitimate purpose, and
- the interference must be a suitable, necessary and adequate measure to achieve the legitimate purpose.

The restriction of the fundamental right must be proportionate in relation to the public interest protected. Furthermore, a provision restricting fundamental rights must comply with the principle of certainty.

When balancing the adequacy of a limitation of fundamental rights and the legitimate aim pursued, the intensity of the limitation must be assessed. The Constitutional Court has developed a set of criteria which indicate the intensity of a fundamental right interference:

- how many bearers of a fundamental right are affected by the measure at question,
- which kind of data is collected; sensitive data[114] or data protected by other constitutional rights like the inviolability of an individuals home or of the mail,
- does the measure involve data fusion or linking of data,
- do subjects of the measure remain anonymous,
- which disadvantage for the individual could the measure result in
- has the data subject given reason to be subject of an investigation or is the investigation carried out regardless of whether the individual is suspected of any wrongdoing

In addition, in the case of surveillance measures the principle of certainty requires that the data subject can realize on which occasion and according to which requirements a certain

[113] BVerfGE 100, 313 (366).
[114] That is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life, Article 8 of Directive 1995/46/EC.

behaviour will result in the threat of surveillance.[115] That way the data subject is able to adjust his behaviour.

However, the court has in a number of cases[116] addressed the view that if uncertainty prevails with regards to whether one's behaviour is monitored and possibly recorded by the government or public authorities, citizens may refrain from pursuing their fundamental rights. The uncertainty is regarded to cause pressure to adjust to the behaviour perceived to be expected.

The Constitutional Court does not hold the view that intensive interference with fundamental rights like privacy is per se unconstitutional. But it regards an intensive interference to be proportionate only if a substantial barrier (*Eingriffsschwelle*) for its execution is complied with. This means the more intensive the fundamental rights limitation, the stricter the threshold has to be.

In his constitutional complaint against the Schleswig-Holstein regulation the appellant holds the view[117] that no sufficient proof of an actual threat to a particularly important right (for example right to corporal integrity, life, and freedom) exists which is protected by the provision permitting ANPR. When analyzing the intensity of privacy restriction caused by ANPR, the criteria developed by the Constitutional Court can be applied.

During ANPR all cars and drivers coincidentally passing the ANPR system's location are affected by the measure regardless of whether they have given any reason for it. The measure is carried out regardless of whether the individual is suspected of any wrongdoing and affects a vast number of vehicle drivers. Even though each recognition may as such not be very intense, the indiscriminate recognition of all citizens passing the system turns ANPR into a very intensive restriction of the right to informational self-determination.

Some police laws allow for covert ANPR. In case of covert ANPR avoiding the monitored roads and locations is impossible for law-abiding citizens. Obligations to notify citizens in case of a "hit" and its further examination are not regulated. If the number of reported false positives hits (up to 40%, see above) is correct, a significantly high number of citizens will face further police measures like searches and interrogations without having given any reason for them.

In a decision passed on 11 March 2008 the Constitutional Court declared the provisions regulating ANPR in the police state laws of Hesse and Schleswig-Holstein void.[118] The court ruled that Article 14 section 5 HSOG and Article 184 section 5 LVwG are violating the German constitution, more precisely the fundamental right of informational self-determination as laid down in Article 2 section 1 and Article 1 section 1 of the Basic Law.

In its opinion the court presents nuanced reasoning concerning different possible constellations of ANPR and their privacy impact.

The first finding of the court concerns the question which of the steps of data processing that are conducted during an ANPR system application do restrict the right of personal self-

---

[115] BVerfG, NJW 2005, 2607.
[116] For example BVerfG, NJW 1984, 422 and BVerfG, DVBl. 2006, 903.
[117] The complaint is available at <www.daten-speicherung.de/data/Verfassungsbeschwerde_Kennzeichen_SH_2007-05-06_anon.pdf>.
[118] The decision is available at <www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr207405.html> (in German).

determination. In a prior decision the constitutional court had ruled that data collection does not constitute a restriction of informational self-determination if the data are "eliminated" (deleted) right after collection without the technical possibility to restore the data if also the data remains anonymous and cannot be linked to any natural person.

In its current decision regarding ANPR the court found that in case of a "no-hit" – if the number plate data is deleted right away and not stored for further processing – no restriction of the right of informational self-determination takes place.

During the court proceeding the concerned German state of Hesse described the technical functionality of the ANPR system used: the ANPR devices used in Hesse contain a temporary memory. The memory size allows for a maximum of nine number plates to be stored at the same time. Number plates stored in this temporary memory are matched with the reference database(s). In case of a hit the picture taken of the number plate is displayed on the laptop screen used to operate the ANPR. It is then possible for the police personnel operating the laptop to manually initiate storage of these data in a permanent memory of the laptop. In case "no hit" occurs the number plate data will remain in the temporary memory of the ANPR device and will be overwritten by new data. This means that only in case of a match with the reference data base the data will be available for further processing by the police authorities.

The court then analysed the lawfulness of this restriction of the right of personal self-determination. A particular characteristic of ANPR lies according to the court in the technically enabled facility to serially check number plates of a big number of cars in a very short period of time. The restriction of the right of personal self-determination is intensified if in addition to the number plate further information is saved, as for example location of the ANPR control, and direction of travel.

The court applied its aforementioned criteria, assessing the intensity of the fundamental right restriction: the court discussed which kind of information is collected and processed, the cause and circumstances of data collection, the category of persons concerned, and the ways of possible data use.

The constitutional court differentiates between two possible aims of ANPR data use. If ANPR is used solely to return stolen cars to their owners and locate the suspected thieves or to detect cars operated without permission as car tax or insurance rates were not paid, the court regards its relevance for the data subject's personality ("Persönlichkeitsrelevanz") to be of less intensity than it is the case for the second possible way of data use. If ANPR is used only to return stolen cars or to detect cars operated without permission as car tax or insurance rates were not paid, then the purpose of number plate recognition is to enable prompt police measures like an immediate search of the located car. Neither conclusions regarding the data subject's behaviour are drawn, nor is a further systematic analysis of the collected data or linking these data with data from different sources carried out in this case.

However, the relevance of ANPR for the subject's personality can increase depending on the location ANPR is used at, and which further information the police holds about data subjects if number plate recognition is indirectly used to analyse the passengers' other behaviour (e.g. participation in political marches). Also if ANPR data is used for further matching with other databases and creation of movement profiles, this purpose is regarded more intense.

The possibility of covert ANPR does increase the fundamental right restriction's intensity, too.

The scrutinized provisions' scope is not sufficiently clear. The regulations lay down that the number plates will be mapped with the existing "search and manhunt data" ("Fahndungsbestand"). Which databases and purposes of storing data for further mapping and access are covered by this term remains not sufficiently clear. Which further measures like for example observation or profiling of citizens can follow and be enabled by ANPR use remains unclear because the scope of data processing and the number and kind of reference databases are not limited and enumerated precisely. The purpose for which data is stored in these reference databases is relevant for the level of privacy implication.

The provisions on ANPR do not comply with the proportionality requirements for fundamental rights restriction. The more intense the regulated restriction of a fundamental right is, the stricter the requirements for a limitation of the conditions are according to the constitutional courts' case law. A very intensive restriction is only permissible in case of sufficient proof of an actual threat to a particularly important right (e.g. the right to corporal integrity, life and freedom). The challenged provisions do not contain the sufficiently precise description of the condition under which a restriction of the fundamental right is permissible ("Eingriffsschwelle"). The purpose of possible ANPR use is not limited and the regulations allow for investigations not based on any suspicion and directed at an indifferent number of citizens ("Ermittlungen ins Blaue hinein")[119]. The constitutional court in several prior cases ruled that these kinds of investigations are unconstitutional.

6.3.6 Legal Aspects of Heavy Vehicles Toll Collection in Germany

The legal basis for heavy vehicles toll collection in Germany is the Motorway Toll Act (*Autobahnmautgesetz* – ABMG[120]) of 12 April 2002, the Regulation Setting the Amount of Toll (*Mauthöheverordnung* – MautHV[121]), the Toll Order (*LKW-Maut-Verordnung*[122]) and the Toll Route Extension Order (*Mautstreckenausdehnungsverordnung* – MautStrAusdehnV[123]). The Motorway Toll Act stipulates the authorization of the German government to lay down the amount of toll by means of regulation. This was implemented by the Regulation Setting the Amount of Toll. The German Toll Order regulates the specific details of truck-toll collection. The Toll Route Extension Order regulates toll collection on selected German trunk roads. These regulations are transposing EU Directive 1999/62/EC on the charging of heavy goods vehicles for the use of certain infrastructure[124]. The Directive was amended[125] by Directives 2006/38/EC and 2006/103/EC. Directive 1999/62/EC harmonises levy systems - vehicle taxes, tolls and charges relating to the use of road infrastructure.

In order to implement the toll collection in Germany, the *Toll Collect* (lega name; Toll Collect GmbH) consortium was funded in March 2002. It is a joint venture of Deutsche Telekom (45%), Daimler, and Cofiroute (Compagnie Financière et Industrielle des Autoroutes, 10%). Toll Collect itself runs the operation of the actual toll collection system for heavy vehicles. Due to several technical problems regarding the complexity of the toll collection systems, the operation of Toll Collect stated 1st January 2005 in a reduced set-up, 16 months later as

---

[119] See margin number 172 et seq. of the decision.
[120] Available in German at <bundesrecht.juris.de/abmg/index.html>.
[121] Available in German at <bundesrecht.juris.de/mauthv/index.html>.
[122] Available in German at <bundesrecht.juris.de/lkw-mautv/index.html>.
[123] Available in German at <bundesrecht.juris.de/mautstrausdehnv/>.
[124] Available at <eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0062:EN:HTML>.
[125] For an overview see <europa.eu/scadplus/leg/en/lvb/l24045b.htm#AMENDINGACT>.

scheduled. The system went fully operational 1st of January 2006. The company's headquarter is located in Berlin (Germany), employing 520 people at the moment. Further information about Toll Collect and its development between 2005 and 2008 can be found in Table 1. Due to current figures 362,797 OBUs are installed in German heavy goods vehicles, followed by Poland (47,894 units), the Netherlands (44,638 units) and the Czech Republic (23,062 units). Over 90% of the tolls collected are by OBU[126].

	01.01.2005	30.11.2007	01.08.2008
On-board units (OBU) rolled out	320.686	608.000	640.000
Cumulated distance of toll-route in billion km	0	75	100
Registered vehicles	532.900	911.000	---
Registered users	70.200	111.100	---
Automated transactions	72 %	90 %	90
Collection rate	> 99 %	99,75 %	99,75

Table 1: Development of Toll Collect between 2005 and 2008.

The obligation to pay toll is laid down for all vehicles or vehicle combinations with a permissible total weight of 12 tons or more and is directed only at goods transport, Article 1 section 1 ABMG. All vehicles moving on German motorways, which meet these requirements must pay toll, regardless of their country of origin. The Federal Office for Goods Traffic (Bundesamt für Güterverkehr – BAG) released the first Toll Statistics in April 2008[127].

The road pricing is conducted based on a classification taking into account the vehicle's number of axles and the emission category as well as the distance travelled. The following table presents the toll rate per kilometre. From September 2008 new rates are valid.

	1-3 Axles	4 and more Axles
Emission Category A	0,0965 Euro	0,1065
Emission Category B	0,1165 Euro	0,1265
Emission Category C	0,1365 Euro	0,1465

Table 2: Toll rates for German motorways

The toll debtor is obliged to enable the toll collection by submitting the required information for pricing, Article 4 section 3 ABMG. The debtor may choose to transmit the information manually, using public terminals at border or truck-stops or by using the Toll Collect Internet website to enrole/sign-up for toll collection. Furthermore he or she can choose to operate so

[126] http://www.roadtraffic-technology.com/projects/lkw-maut/
[127] More information is available at <www.bag.bund.de/cln_009/nn_46210/DE/VerkehrsThemen/Statistik/Mautstatistik/mautstatistik.html>.

called on-board units (OBUs) allowing for an automatic enrolement and toll calculation for a vehicle. The two enrolement / sign-up processes are further visualised in the following Figure:

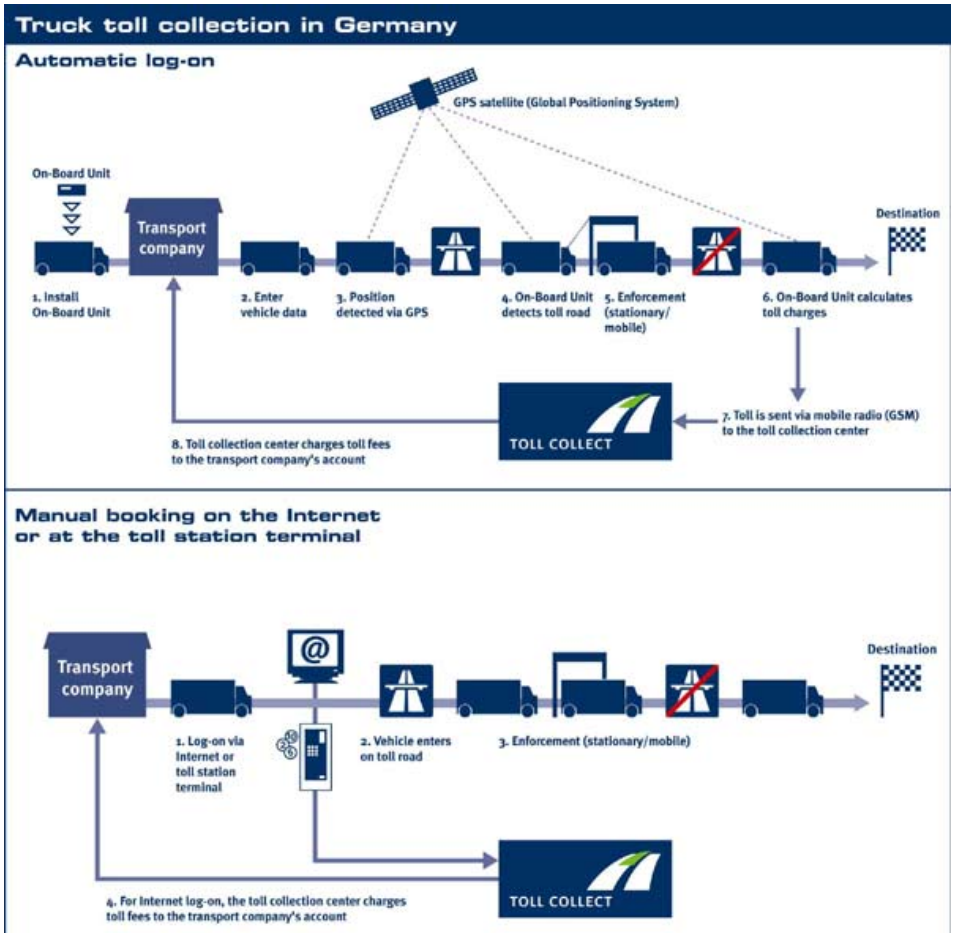

Figure 1: Sign-up/Enrolement Process for Toll Collect[128]

Data required for charging the toll covers (Article 3 LKW-Maut-V):

- number plate of debtor,
- nationality plate,
- distance travelled,
- date and time of planned start,
- number of axles,
- emission class.

In order to enable checks of lawful submission of the required data additional data may be collected and processed by the Federal Office for Goods Traffic, the private operator of the toll collection system Toll Collect GmbH, and the customs office according to Article 7 section 2 ABMG:

- picture of the vehicle,

[128] Cf. http://www.roadtraffic-technology.com/projects/lkw-maut/lkw-maut4.html

- name of the vehicle driver,
- location and time of motorway use,
- number plate of the vehicle,
- number of axles,
- emission class.

In addition 300 toll checker gantries strategically are located throughout the country, Toll Enforcement also relies on mobile patrols, consisting of a fleet of 300 vehicles with 540 officers of the Federal Office of Freight (BAG). The officers patrol the German motorways, checking vehicles and drivers to see if they have paid the toll or have the OBU installed (these vehicles will be equipped with an infrared short range DSRC (Dedicated Short Range Communications) system that can be used to scan and monitor trucks in motion). The BAG has police powers to request trucks to stop for examination at any point during their journey.[129]

6.3.7 Function creep – Legitimacy of using toll collection data for law enforcement purposes

These data processed and used during the toll collection process can be aggregated to comprehensive profiles regarding the movements of the vehicles and their drivers. For this reason law enforcement authorities have sought to get access to toll collection data. In a decision in 2003 the County Court Gummersbach decided[130] that Toll Collect GmbH was obliged to transmit toll collection data to the law enforcement authorities investigating a specific case.

Scholars discussed this decision controversially, because the Motorway Toll Act contains a distinct provision on the scope of permissible data processing and data use in Article 4 section 2 sentence 3.[131] According to this regulation "these data may only be processed and used for the purpose of this law". The provision permits data processing and use by the Federal Office for Goods Traffic, the private operator of the toll collection system Toll Collect GmbH, and the customs office.

Taking into account the precise wording as well as the legislative intent stated in the statement of reasons[132] for legislation of the ABMG even the German minister of the interior Wolfgang Schäuble points out that the ABMG currently contains a "strict purpose binding" provision not permitting exceptions[133]. Hence using toll collection data for law enforcement purposes is not permissible under the current legal framework.

The minister of the interior, Wolfgang Schäuble, has repeatedly stated his view that the provision containing the purpose limitation needs to be amended to allow access for law enforcement authorities.

---

[129] See http://www.roadtraffic-technology.com/projects/lkw-maut/

[130] AG Gummersbach, Beschluss vom 21.8.2003 – 10a Gs 239/03.

[131] See Göres, U., 2004, *Rechtmäßigkeit des Zugriffs der Strafverfolgungsbehörden auf die Daten der Mauterfassung*, Neue Juristische Wochenschrift No. 4/2004 and Pfab, A., 2005, *Rechtsprobleme bei Datenschutz und Strafverfolgung im Autobahnmautgesetz*, Neue Zeitschrift für Verkehrsrecht No. 10/2005.

[132] BT-Dr 14/7013, page 14.

[133] Schäuble, W., 2007, *Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts*, Zeitschrift für Rechtspolitik No. 7/2007.

6.3.8 Conclusion

Existing legal provisions regulating the use of APNR as an investigational means were ruled unconstitutional by the German Constitutional Court. Reported figures of hits during trials carried out in the German state of Schleswig-Holstein raise doubts regarding the effectiveness of ANPR use. Scanning 131.000 number plates returned 26 hits, all of them concerning cars for which car tax or insurance rates were not paid. No stolen car was detected.[134] Schleswig-Holstein's Home Secretary Lothar Hay called this result unproportional, considering the privacy infringement caused by APNR. Not all German states have joined this opinion and will refrain from allowing APNR use in the future.

[134] See NDR, Kennzeichenscanning verfassungswidrig. Available at http://www3.ndr.de/ndrtv_pages_nimex/0,3601,SPM2468_URLaHR0cDovL3d3dzEubmRyLmRlL25hY2hyaWNodGVuL2tlbm56ZWljaGVuc2Nhbm5pbmcyLW5pbWV4ZGV0YWlsLnhtbA==,00.html.

6.4 Germany: Case 2 - Mobile Identities and Electronic License Plates

6.4.1 Introduction

Traditional license plates for cars effectively provide an identifier, i.e. an identity, to a car. They provide a link to the owner of the car by use of a data base storing this information, where the identifier on the license plate is the key. Furthermore, as the identifier is fixed, it is trackable.

While these identifiers are human-readable, using them for automatic identification of cars requires considerable technical effort. Automatic devices for license plate reading contain delicate optical systems as well as advanced processing systems for optical character recognition. Furthermore, the aspect of tamper-resistance and fraud protection needs to be considered. It is well-known that criminals make use of stolen or faked license plates to hide their identities.

In this situation, the use of established technology for wireless transmission of car identifiers has been proposed. Some of these proposals are undergoing field trials or are already in day-to-day use. Examples are described in more details below.

While electronically, especially wirelessly, readable license plates provide the possibility of easier collection of car identifiers, they allow further usage scenarios like general or location specific road tolls. Especially interesting in this respect is the RFID technology in a broad sense.

In the remainder of this section we first describe the RFID technology along with relevant security aspects, then we discuss examples of proposed system.

6.4.2 Radio Frequency Identification (RFID)

The term RFID refers, in general, to a technology that uses small wireless devices for the purpose of identifying physical objects, e.g. a container.

Usually, an RFID system is comprised of a number of transponders and readers. The connection between a reader and a transponder is achieved by wireless communication using a suitable protocol. A transponder, also called a *tag*, is directly connected to some physical object while the reader is the instance that receives the identification information of the transponders in range.

While in a narrow sense RFID refers to wireless object identification, like electronic product codes, the technology itself can give rise to a number of different application scenarios, which include also transmission of information about objects or even information in general. A prominent example is the RFID-based passport, where the physical identification of the passport itself is not the primary goal, but rather obtaining some data about the legitimate bearer of the passport.

RFID systems can be classified along a number of dimensions:

- Power supply for the transponder: The transponder can be *active*, i.e. include a separate power supply like a battery, or *passive*. A passive transponder is powered by tapping the electro-magnetic field supplied by the reader.

- Communication range: This ranges from several centimetres to several meters for some passive transponders, up to several tens of meters for active transponders.
- Computing and storage capabilities of the transponder: While very basic transponder types store only about 96 bits of data without much further processing capabilities, other types offer sophisticated processing options and access control features, also ranging to the possibility of cryptographic operations, and several ten of kilobytes of storage.
- Communication interface and standard: This dimension primarily addresses the operating frequency of the communication interface (low frequency LF, high frequency HF, ultra high frequency UHF), having an impact on the transmission bandwidth as well as the communication distance, e.g. tens of centimetres for passive HF transponders to several meters for passive UHF transponders. This dimension also has a strong impact on the amount of available power for passive transponders.

Not all possible combinations are available, and some combinations are not possible using existing technology. For example, passive transponders providing strong cryptographic functions are, with current technology, only available for the HF interface, which strongly limits the communication range.

Further material on RFID systems, their functionality, and possible risks and attacks are covered, e.g., in Security Aspects and Prospective Applications of RFID Systems.[135]

It should be noted that transponders useful for electronic license plate applications are basically those with a communication range of several meters. As a consequence, with currently available technology, passive UHF transponders as well as active transponders are the most suitable. However, while active transponders could be manufactured to include advanced security measures, passive UHF transponders are not available with reliable, strong security mechanisms except permanent write protection.

6.4.3 Examples of Proposed and Existing Systems for Electronic License Plates

In the sequel some examples of electronic license plate systems are reviewed. Further, some electronic road toll systems based on RFID technology are described.

- iltag – Intelligent License Tag, also named “third license plate” (Utsch AG)[136] [137]: This proposal is based on passive HF transponders to be placed on the inside of the wind screen. While the used transponder does offer several separated storage partitions that can be protected by individual passwords, the HF technology severely limits the communication distance, such that the system can only operate if reader and transponder are in rather close proximity.

---

[135] Federal Office for Information Security. Security Aspects and Prospective Applications of RFID Systems, <www.bsi.de/fachthem/rfid/RIKCHA_en.htm>.

[136] D. Adamczewski. Digitales Nummernschild für Kraftfahrzeuge. Heise Online, June 12, 2001, <www.heise.de/newsticker/meldung/18421>.

[137] K. Kleinau. Drittes Auto-Kennzeichen schreckt vor Autodiebstahl ab. Innovations-Report, September 17, 2002, <www.innovations-report.de/html/berichte/informationstechnologie/bericht-12938.html>.

- Electronic Vehicle Registration (3M)[138] [139]: This system is installed in Bermuda to help relieve problems with non-licensed cars. The transponders are passive UHF transponders, such that the system can reach communication distances of several meters. This allows automatic data retrieval at road crossings etc. The transponders contain only a unique identification number, while the accompanying data is stored in a data base, indexed by the transponder's identification number.
- e-Plate (Hill Number Plates Ltd.)[140] [141]: This system is based on an active transponder integrated into the physical number plate. The transponder is powered by a battery and is claimed to have a life time of up to 10 years. The transponder contains a unique identification that is transmitted in short intervals, i.e. interactive protocols between reader and transponder do not exist. The communication range is claimed to be up to 100 meters.
- Electronic Number Plate (IPICO)[142]: For this system, a special type of transponder is used that employs non-standard communication protocols ("transponder talks first" instead of the usual "reader talks first"). Effectively, the transponders can be seen as UHF transponders, such that the communication range is about 2 to 7 meters. Each transponder contains a unique 64-bit number plus 192 bits of additional information. No further security functionality is offered by the transponders.

From these examples it can be seen that in current systems the transponders effectively attach an electronically readable serial number to the bearing cars.

6.4.4 Privacy issues with Electronic License Plates

Having seen in section 6.2.11 the necessary technical details, this section deals with the privacy issues that result from using these or similar proposals. Further security issues, like cloning of RFID tags, etc., are ignored in the following.

In fact, as noticed above, a traditional license plate provides a fixed identifier for the car the license plate is issued for. This identifier is fixed during the lifetime of the license plate, and is clearly visible[143]. With all proposals described above, the situation basically stays the same; the car carries a fixed electronic identifier. However, there is a huge qualitative difference here.

The traditional license plate can only be read out optically. This is, most of the time, easy for the human eye, but requires considerable technical effort to do automatically in large numbers. Nevertheless, such equipment is already deployed. For example, in Germany, the road toll system for large trucks makes use of bridges above the motorways that routinely use optical character recognition in order to check if a truck passing by does not evade paying the

[138] R. Wessel. Bermuda's RFID Vehicle Registration System Could Save $2 Million/year. RFID Journal, May 18, 2007, <www.rfidjournal.com/article/view/3321/>.
[139] P.-M. Ziegler. Bermuda startet RFID-gestütztes Verkehrsüberwachungssystem. Heise Online, May 9, 2007, <www.heise.de/newsticker/meldung/89504>.
[140] e-Plate website, <www.e-plate.com>.
[141] Wikipedia: e-Plate, <de.wikipedia.org/wiki/E-Plate>.
[142] IPICO. IP-X Read-Only UHF RFID Tag – Electronic Number Plate (ENP). March 9, 2007, <www.ipico.com/site/iPico_100/pdf/IP-PROD-XTRO-170x10ENP-20070309.pdf>.
[143] As required by law.

toll. Another example is the use of mobile number plate scanners by the police.[144] Nevertheless, a whole-sale approach to license plate reading and tracking of traditional optical license plates is not easily implemented.

With the described proposals for electronic license plates, each car has a unique identifier that is electronically readable using off-the-shelf equipment, which makes it additionally rather cheap and easily obtainable for anyone. This has consequences in two directions: one is that automatic mass surveillance and tracking becomes, on a technical level, vastly easier than before with optical license plates, and the other is, that automatic tracking of individual or specific cars becomes not only technically feasible, but essentially easy for basically everyone interested.

Examples are due to potential problems arising from these consequences:

1. Automatic mass surveillance: Consider a series of demonstrations in favour of the political opposition. Obtaining the electronic identities of cars entering a town the days before a demonstration, and correlating these with those identities collected during similar event allows to build up a database of cars that should be further identified and linked to their owners, given rise to the suspicion that the owner of the respective cars belong to a "core" of the movement.
2. Automatic tracking by individuals or private organisations: Obtaining the identities of cars driving or parking near a city's red light district could lead to a database of potential targets for black mailing. Correlating this database with cars found in the more expensive areas of the city sorts out the "interesting" targets. The potential for similar criminal activities should be obvious.
3. Automatic tracking: Once the unique and fixed electronic identity of a car is linked to its owner, a reader can be used to trigger a bomb selectively for only one person. There will be no further need for the criminal to actually attend the crime scene once the trigger is installed.

From these examples, admittedly rather extreme, it can be seen that attaching a fixed, electronically readable identifier to cars can lead to very serious consequences regarding privacy.

6.4.5 Review of Scientific Proposals

The privacy issues elaborated in the previous section have, at least in part, been addressed in scientific literature. This section contains a review of the most important scientific proposals to remedy these privacy issues. A survey of the status of research is available from [Ju2006]. We limit ourselves to passive RFID tags here, as these appear to be, from the communication range point of view, the most suitable for electronic license plates. Some of the most important proposals shall be discussed below:

- *Temporary deactivation of tags*: Juels[145] proposes to deactivate RFID tags so that unauthorized readers cannot access the tags. This requires a reactivation mechanism

[144] Note, however, that there is a legal dispute going on about the use of this technology.
[145] A. Juels. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications 24(2):381-394, 2006. An earlier version is available from <www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf>.

involving some form of access control, like a PIN. However, for a large number of tags all authorized readers need to know all PINs, so that a trade-off between the number of PINs and the security against leaks is necessary. Further, the PIN could be derived or looked up using the optically readable license number of the car (or some additional bar code etc.). However, this would require obtaining this number for every single legitimate read-out of the respective tag.

- *Pseudonyms*: In Minimalist *Cryptography for Low-Cost RFID Tags*[146] Juels proposes to issue a number of pseudonyms to each tag. The tag would then select one of the pseudonyms upon activation. Usually, an unauthorised reader would not know all pseudonyms of a tag; therefore, linking a number of sightings of the same tag would be difficult. Authorised readers could also update the set of pseudonyms for a given tag. However, with this proposal, all authorised readers need to know all pseudonyms of all tags, or at least have access to a database containing them.
- *Re-encryption of tag data*: Juels and Pappu propose in *Squealing Euros : Privacy Protection in RFID-Enabled Banknotes*[147] a system, where after each successful read-out of a tag by an authorised reader, the contents of the tag is re-encrypted and stored in this new form on the tag. The concrete proposal in *Squealing Euros* aims at embedding RFID tags in bank notes, but in such a way that obvious privacy problems with tracking and leaking of how much money someone has in his wallet are avoided. However, this system would require that the tags can recognise authorised readers and prevent unauthorised readers from changing or destroying the data stored on the tag. Given the minimalist security functionality present on current passive UHF tags, this proposal seems not to be viable for car license plates if privacy issues shall be taken into consideration.
- *Randomisation of tag data*: A similar idea has been proposed by Ateniese, Camenisch and de Medeiros[148]. Here, the normal readers do not rewrite a tag's contents. Instead, a *randomiser* is introduced with the sole purpose to transform the encrypted data stored on the tag into another encrypted instance of the same data, but without ever decrypting the data. Thus, a randomiser does not obtain any secret information. While this proposal can address the privacy issues if enough randomisers are deployed, the problem of a writable tag is still present. Thus, a denial of service attack is still possible where the data stored on the tag is not randomised, but destroyed.
- *RFID-Proxies*: An RFID-Proxy is a device that acts as an intermediary between reader and tag, and can control which reader can interact with which tag. There are several proposals in the literature, like *A Batterypowered Mobile Device for RFID Privacy Management*[149], and *High-Power Proxies for Enhancing RFID Privacy and Utility*.[150]

---

[146] A. Juels. Minimalist Cryptography for Low-Cost RFID Tags. International Conference of Security in Communication Networks (SCN), 2004.
[147] A. Juels, R. Pappu. Squealing Euros : Privacy Protection in RFID-Enabled Banknotes. Financial Cryptography (FC), 2003.
[148] G. Ateniese, J. Camenisch, B. de Medeiros. Untraceable RFID Tags via Insubvertible Encryption. Proceedings of the 12th ACM Conference on Computer and Communication Security (CCS), pp 92-101, ACM Press, 2005.
[149] B. Crispo, M. Rieback, A. Tanenbaum. RFID Guardian: A Batterypowered Mobile Device for RFID Privacy Management. In C. Boyd, J. M. Gonzáles Nieto (eds), Proceedings of the Australasian Conference on Information Security and Privacy (ACISP), Lecture Notes in Computer Science volume 3574, pp. 184-194, Springer-Verlag, 2005.

Such a proxy can run sophisticated cryptographic protocols, thus alleviating the privacy issues raised above. However, the issue of how to put a tag under a proxy's control and how to remove it again is still open. Further, if it appears suitable to include an RFID proxy into a car, then, with the same arguments, active transponders with enough computing power would appear suitable for inclusion, too.

- *Trusted Computing*: The proposal of Molnar, Soppera, and Wagner [no reference below MSW2005] involves a trusted platform module (TPM) that is included in every authorised reader. This TPM can verify that the reader has not been tampered with, and only release keyed needed for reading a tag's data if this is the case. Further, the reader would then, also TPM-enforced, stick to an explicit privacy policy. Unless the tags contain some cryptographically strong access control, however, this approach still does not solve some of the privacy issues. While the tag data might be encrypted, so that unauthorised readers cannot obtain the cleartext data, they could still obtain an opaque, but unique bit string from the tag. Thus, even an unauthorised reader could re-identify a car once it knows the correspondence of the tag data and the license number, resp. car or owner identity.

In total, it turns out that the proposals made in the scientific literature do not all address the privacy issues that arise when employing simple passive RFID tags for electronic license plates. Other approaches, i.e. using active transponders that are built into cars might be viable, provided that suitable strong cryptographic protocols are employed.

6.4.6 Conclusion

Employing RFID-based or otherwise electronic license plates to cars raises a number of privacy issues that need to be addressed before such a system should be deployed.

The discussion above about the current state of the art with respect to privacy regarding passive RFID transponders highlights that there is still a long way to go before passive transponders to be employed. The problem here is that so far, one can have either strong cryptography or a large communication range, but not both. But having both is a prerequisite for a usable electronic license plate system that offers its promised advantages without the identified privacy issues.

Nevertheless, in the car application scenario there is no real need to rely on passive, minimal-power RFID transponders, as sufficient energy is easily available. Therefore, it appears that an integration of more powerful, active transponders into cars seems advisable, such that both a useful communication range as well as strong cryptographic protocols can be implemented. Indeed, both aspects are necessary to have a usable, secure system.

6.5 Germany: Case 3 - Mobile Identities and Car Telematics

[150] D. Bailey, A. Juels, P. Syverson. High-Power Proxies for Enhancing RFID Privacy and Utility. In G. Danezis, D. Martin (eds), Proceedings of Privacy Enhancing Technologies (PET), 2005.

6.5.1 Introduction

Traffic telematics services are already being integrated into some high end cars. The purpose of this section is to review how such a service works. Here we use the example of the BMW ConnectedDrive car telematics service.[151] Special attention will also be placed on the privacy aspects of this service. Here, privacy not only means the privacy of data, but also includes the position of a car at a given time. We will call the latter aspect also "location privacy".

6.5.2 System overview

The BMW ConnectedDrive service is briefly described in [BMW2008]. It consists of a portfolio of five services, of which three are of interest here:

- BMW Assist: This service offers traffic information to the driver, in addition to an emergency call feature activated by crash sensors. Roadside sensors collect information about traffic jams. The collected information is made available to the cars' navigation system. In fact, in order to use this information, the car sends its current position as obtained through GPS to the service's server and receives the relevant information on traffic conditions.
- BMW Online: This service provides localised internet services by coupling a search engine with location information (Google local search). Here, the car's position is used to localise the search results. The connection is done using GSM/EDGE, so that the car effectively has an identity provided by the GSM SIM.
- BMW Tracking: This service allows tracking a car in case of theft. Either the owner reports the theft, in which case the tracking system is switched on remotely, or the car's anti-theft system activates it automatically. In the latter case, the central service tries to validate the alarm by contacting the car's owner.

6.5.3 Privacy Issues

The information available from the *BMW ConnectedDrive Introduction* does not contain any hint on any use of special technology for special handling of location data to provide privacy to the cars' users. In fact, the lack of this information could be seen as a hint that such technology is not in use. The following discussion is based on this assumption.

The service for providing traffic condition information to the driver apparently transmits the position in intervals to a central server, so that this server obtains all positions of all cars subscribed to the service. This information would allow tracking all these cars regularly, at least by the server itself and any entity with access to the position data. In fact, this collection can be a huge and valuable target for an adversary. Apparently no further privacy enhancing technology is used like blinding the identity of the car, or the use of a location intermediary as

[151] BMW ConnectedDrive Introduction. Online at <www.bmw.com/com/en/insights/technology/connecteddrive/overview.html>.

proposed, e.g., in Enabling Privacy of Real-Life LBS[152] and Privacy-Friendly LBS: A Prototype-Supported Case Study.[153]

The same issue seems to be present with the online search service. Here the position information is provided along with search queries. Apparently, a central service is used as a communication endpoint and relay to the internet, so that this server obtains the car's identity by its GSM phone number, as well as the search query and the location information. Such data is even more privacy-invading than the traffic condition service just discussed, as here special interests and topics are provided by the search queries.

In case of theft, the automatic tracking system is certainly a very useful service; however, it is not fully clear how the remote activation works. Certainly, the protection against malicious activation needs attention, as well as the way the destination of the position information is set in the car's system. If these features are not strongly protected, an adversary might activate the automatic transmission of the car's position. It is a design feature that the activation cannot be noticed by the car's user (otherwise this would create an incentive for a thief to shut it down). Furthermore, if the recipient of the position information can be changed by unauthorised persons, e.g. by changing the telephone number of the recipient, this system would provide a well-hidden tracking system in case of abuse.

For correctness sake, it should be highlighted again that the web site *BMW ConnectedDrive*[154] does not address if and how any of these issues are resolved by technical or organisational methods.

6.5.4 Intermediaries for Location-Based Services

As location information is very sensitive with respect to privacy, proposals have been made to remedy the problem that location information must be given to a service provider in order to be able to have location-based services at all. The privacy issues stem from both location and identity information being available at the same time.

One such proposal[155] – although in the context of GSM or mobile telephone systems – is based in trusted intermediaries that mediate between the user, the service provider, and the location provider. Here, a trusted intermediary obtains, upon request by the user, location information from the mobile operator, and translates the user's identity into a pseudonym which is given to the service provider along with the user's position. Here, the intermediary ensures that the mobile operator does not know what service the user requests, while the service provider does not know the user's identity. A prototype of such a system has been implemented. It is described in *Privacy-Friendly LBS: A Prototype-Supported Case Study*.[156]

It is conceivable that this idea can be adapted to design a system in a similar fashion where the location information is provided by the user itself.

---

[152] J. Zimbuschka, L. Fritsch, M. Radmacher, T. Scherner, K. Rannenberg. Enabling Privacy of Real-Life LBS. Proceedings of the 22nd IFIP TC-11 International Information Security Conference IFIP Sec 2007, IFIP International Federation for Information Processing Series Vol. 232, pp. 325-336, Springer-Verlag, 2007.
[153] J. Zimbuschka, L. Fritsch, M. Radmacher, T. Scherner, K. Rannenberg. Privacy-Friendly LBS: A Prototype-Supported Case Study. Proceedings of the 13th Americas Conference on Information Systems, 2007.
[154] See note 147.
[155] See note 148.
[156] See note 149.

6.5.5 Conclusion

We have examined an example of a location-based car telematic service. Here, a car has an identity in order to participate in the service. This, however, does lead to privacy issues as the service provider does obtain both the position – location information – as well as the car's identity, which has a direct link to the owner's and possibly the user's identity. Furthermore, we have reviewed a possible method to separate location and identity information in order to resolve the privacy issues involved in the current design.

6.6 Sweden: The Stockholm Congestion Tax System

6.6.1 Introduction

In 2003 the Swedish Parliament decided to do a full scale experiment on a Road Toll System for the Stockholm City area. The purposes of the experiment were the following:[157]

1. more effective use of the road system by reducing the traffic load.
2. reduce the number of choke points and increase the mean speed.
3. improve the city environment by reducing the emission and noise and by doing this enable more housing areas.
4. (in the long run) achieve further environmental improvements by stimulating a transfer to more environmental friendly vehicles and fuels

The experiment was supposed to start at the end of 2004 and the project was to be lead by the city council of Stockholm city and the responsibility for the implementation and administration of the system was given to the Swedish Road Administration (Vägvärket). However, due to a number of complaints from citizens and council members regarding the validity and legality of the decision it was delayed. The actual implementation of the system was further delayed by complaints by some of the bidders in the acquisition process that felt that the process was not conducted in the proper way. These issues were finally settled and the toll system experiment was put into operation on the 3rd of January 2006 and finished on the 31st of July 2006. The experiment was evaluated and summarized in a report that was published in the summer of 2006. [158]

The 17th of September 2006 a referendum on Road Tolls was held in the Stockholm area and based on this referendum the Road Toll system was permanently put into operation on the 1st of August 2007.

6.6.2 Overview of the system

This section contains a very high level overview of the system. A more detailed description can be found in literature.[159] The system consists of a number of toll stations spread over the Stockholm city area and a backend system. The toll stations (see figure 6.2) in turn comprises of laser detectors (B), antennas (based on the Dedicated Short Range Communications (DSRC) system) (C) and cameras (A and D). When a vehicle activates the laser detector the cameras takes a picture of the front and rear number plates. The pictures are taken using infrared light and in essence the only thing showing up on the picture is the number plate. The camera performs an optical character recognition (OCR) scan of the picture and the registration number is identified. If the vehicle is equipped with a transponder the transponder will communicate with the antenna. The data is then sent to the backend system and stored.

[157] Miljöavgifter i Stockholm - Analys av effekter av olika förslag till utformning, Huvudrapport Transek 2003-12 <www.stockholmsforsoket.se/templates/page.aspx?id=12556>. The authors translation.
[158] Fakta och resultat från Stockholmsförsöket. Analysgruppens sammanfattning - andra versionen augusti 2006 <www.stockholmsforsoket.se/templates/page.aspx?id=8432>.
[159] Vägverket, SCTP Business Requrements Specification.

The data that are sent include the picture, the registration number, the date and time of passage, which station that was passed and the amount charged.

Very few vehicles are currently equipped with transponders. During the test phase transponders were used in order to strengthen the authentication when automatic payment was used as an extra precaution. However, in the current system the technology in the camera is reliable enough (according) to the Swedish road administration so the transponder is not needed for that purpose. Therefore, in the current operation of the system transponders are only used on vehicles liable for the so called "Lidingö rule"[160].

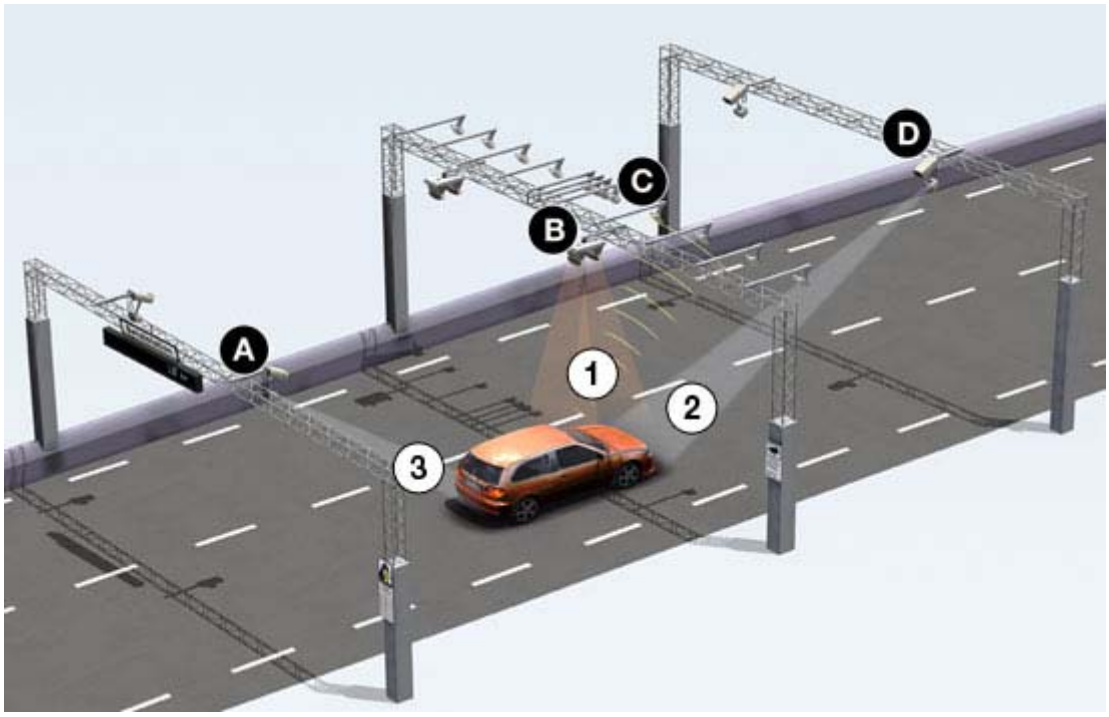

Figure 6.2: The anatomy of a pay station[161]

6.6.3 Privacy and security considerations

Due to the legal framework in Sweden the payment charged at the payment station has to be a tax. Thus, a tax decision is needed for every passage. This tax decision is stored together with the before mentioned data i.e. the picture of the number plate, the registration number, the date and time of passage, which station was passed and the amount charged.

[160] Lidingö is an island that is part of Stockholm and the only roads leading in and out of the island goes through the city center. Thus, people living in Lidingö (or for one reason or another need to travel there frequently from outside of the city) are not charged if they enter and exit the toll zone within 30 minutes (one of the pay stations passed needs to be located close to the Lidingö bridge).
[161] Vägverket, Betalstationen- så fungerar den. <www.vv.se/templates/page3wide____21311.aspx>.

This data is considered public[162] except for the time of passage and pay station passed. These two are considered secret and are only handed out, on request, to the owner of the vehicle by traditional mail.

Under normal circumstances (i.e. the tax is paid in time) the data is deleted 28 days after payment and late payers are deleted 67 days after payment. Data on vehicles that are exempted from tax or where a positive identification is not possible are deleted one day after passage. The system has the possibilities of manually exempting records from deletion by setting a do-not-delete-flag on the record.

There is also the possibility of anonymizing the data instead of deleting it for reporting and statistical purposes.

The system has quite stringent security requirements that are described in Almer et al. Data are protected by role-based access control and protected logs are used to trace actions. These logs are periodically reviewed by security officers. All outside transfers are protected by secure sockets layer (SSL) and network intrusion detection is used. The whole system is required to adhere to the ISO 17799 standard.[163]

For persons with protected identities special procedures are in place and they are only handled by specially authorized personnel.

As far as function creep is concerned, the collected information is not used for anything else than tax decisions. However, the information being collected is classified as secret, but it can be handed out to the police on suspicion of a criminal action. Secret information can be handed out to the prosecutors office, the police or any other authority that have the responsibility to act on a crime, if somebody is under suspicion and imprisonment is constituted for the crime and that the actual crime can be assumed to give a stronger consequence ("in court") than a fine.

6.6.4 Privacy concerns

The person liable to the tax decision is the owner of the car and thus some of the processing mentioned in section 6.3.4 is done in order to find the personal details of the owner. However, the database used for this purpose is the Swedish Car Register which to a large extent also is a public register (see: <https://www21.vv.se/fordonsfraga/>) from which some data are available on line and others can be retrieved through sms, phone or fax . Thus it is not hard for anybody to get information on the owner or the car given the registration number.

The information on the tax decision is as mentioned before considered as public. The tax decision contains information on dates and amounts charged. All roads going in or out of the Stockholm city area are monitored giving a total of 18 toll stations. A car is registered either leaving or entering the Stockholm city area between 06.00-19.00 Monday-Friday and the amount charged is different depending on the time of passage. Three amounts are charged 10, 15,and 20 SEK. Thus because of the difference in charging it is theoretically possible in the worst case to deduce from the tax decision that a car entered or left the Stockholm city centre within a time span of around an hour either in the morning or in the afternoon (the 20SEK

[162] Public data in Sweden can be (and generally must be) given to anyone that asks for it. The data is usually provided through paper printouts but are in some cases accessible through web-pages or sms-services.
[163] ISO/IEC 17799, Wikipedia <de.wikipedia.org/wiki/ISO_17799>.

charge is for passage 07:30-08:29 and 16:00-17:29, the 15 SEK for passage 07:00-07:29, 08:30-08:59, 15:30-15:59 and 17:30-17:59, and the 10 SEK charge is for the rest of the time between 06.30 -18.30). Thus, there is a very limited and quite fuzzy information that can be deduced other than the fact that the car has been in the city centre at some time during the day.

As far as function creep is concerned, the collected information is under usual circumstances not supposed to be used for anything else than tax decisions. However, even though the information being collected is classified as secret, but it can be handed out to the police on suspicion of a criminal action. Secret information can be handed out to the prosecutors office, the police or any other authority that have the responsibility to act on a crime, if somebody is under suspicion and imprisonment is constituted for the crime and that the actual crime can be assumed to give a stronger consequence ("in court") than a fine.

6.6.5 Conclusion

The Stockholm Congestion Tax system was installed for traffic regulation and environment protection purposes. However, the data that are collected allow deriving detailed movement profiles of car holders and therefore pose privacy risks. For protecting the data and preventing their misuse for other purposes such as surveillance, stringent technical and organisational security and privacy measures have been implemented. Still, as discussed in this chapter, some privacy concerns remain, as information on tax decisions is public information in Sweden, and as under certain circumstances the traffic data might also be used for law enforcement purposes.

Such privacy concerns could have been avoided if an alternative anonymous payment system that does not require to collect personal traffic data would have been implemented instead.

6.7 The Netherlands: Kilometerprijs

6.7.1 Introduction

After lenghty discussions in and outside parliament, and after piles of reports finally The Netherlands has chosen for a road pricing system, which not only should prevent a so-called traffic infarct to occur, but which also introduces a transparent and fair paying system. The system is called Kilometerprijs. In this case study – after a short description of Dutch traffic monitoring history – the system of Kilometerprijs and it's possible impact on privay issue id described.

6.7.2 History of traffic monitoring in The Netherlands

To prevent a traffic infarct to occur in The Netherlands and to distribute the financial burden more honestly amongst users governments in a row have been discussing the introduction of another way of paying for mobility for years now. The first system on the drawing table was called *Rekeningrijden*.[164] Simply said, this was a system of electronic gateways around the big cities, which should coerce people to travel to the cities in other way than by car and/or at another moment of the day avoiding rush hours. The system was mainly aimed at diminishing traffic jams during peak hours in the mornings and evenings.
It was similar to those of London and Stockholm (see the case study of the Stockholm Congestion Tax System). However, the Dutch system didn´t make it much further than a few experiments after which the government decided to stop the development of *Rekeningrijden*. A few gateways can still be seen along a few motorways.

One of the great opponents of *Rekeningrijden*, the former head of the Dutch automobile association, later became chairman of the *Nationaal Platform Anders Betalen voor Mobiliteit*, a national platform for research and discussing other ways of paying for mobility. This platform has written an advice on new ways for paying for mobility in 2005.[165] On the same topic the report *Starten met de Kilometerprijs* has been written in 2007.[166] Those studies have lead to the de
cision that in The Netherlands a new payment system for using roads will be introduced: *Kilometerprijs*. At least, that is what the present government is heading for. [167]

6.7.3 The system of Kilometerprijs

The system of *Kilometerprijs* will result in civilians not paying for possessing a vehicle, but for using it. Present taxes involved in possessing and using vehicles will be reduced and abolished and people are going to pay per kilometer. Who drives a little pays a little, who drives a lot pays a lot. But not only that, one has to pay more if one possesses and uses a vehicle which is a greater burden to the environment and/or if one uses certain roads during certain periods of a day (peak hours). And in contradiction to *Rekeningrijden* the system

---

[164] File Rekeningrijden, NRC Handelsblad <www.nrc.nl/W2/Lab/Rekeningrijden/>.
[165] Report Nationaal Platform Anders Betalen voor Mobiliteit, see website of the platform, (<www.andersbetalenvoormobiliteit.nl> click the button *Advies*).
[166] Starten met de kilometerprijs. Overzicht van voorbereidend onderzoek bij
het kabinetsbesluit over de kilometerprijs., Ministry of Transport, Public Works and Water Management. The report is available on the website of the ministry, <www.verkeerenwaterstaat.nl>. Click *Mobiliteit en bereikbaarheid* and next click *Anders Betalen voor Mobiliteit.*
[167] Kabinet geeft gas op weg naar invoering kilometerprijs, Ministry of Finance, 30 May 2008 (<www.minfin.nl> search for *kilometerprijs*).

Kilometerprijs will not be used only in the busy areas in The Netherlands, but in the whole country.

For the system of Kilometerprijs the government has studied several technologies. In the end is chosen for a satellite navigation system (gps/Gallileo) in every vehicle combined with telecommunication facilities (gsm/GPRS) for transport of travel data to a computer centre. The latter is necessary for billing. Herewith calculation of the price to be paid can take place in the vehicle after which the data are sent to the computer centre for administrative affairs, or the travel data are transported to a computer centre and are being calculated then. It is obvious that the latter option can have a greater impact on privacy than the first. After all, using the first option the travel data stay in the vehicle. This is what the Dutch Data Protection Commissioner prefers.[168]

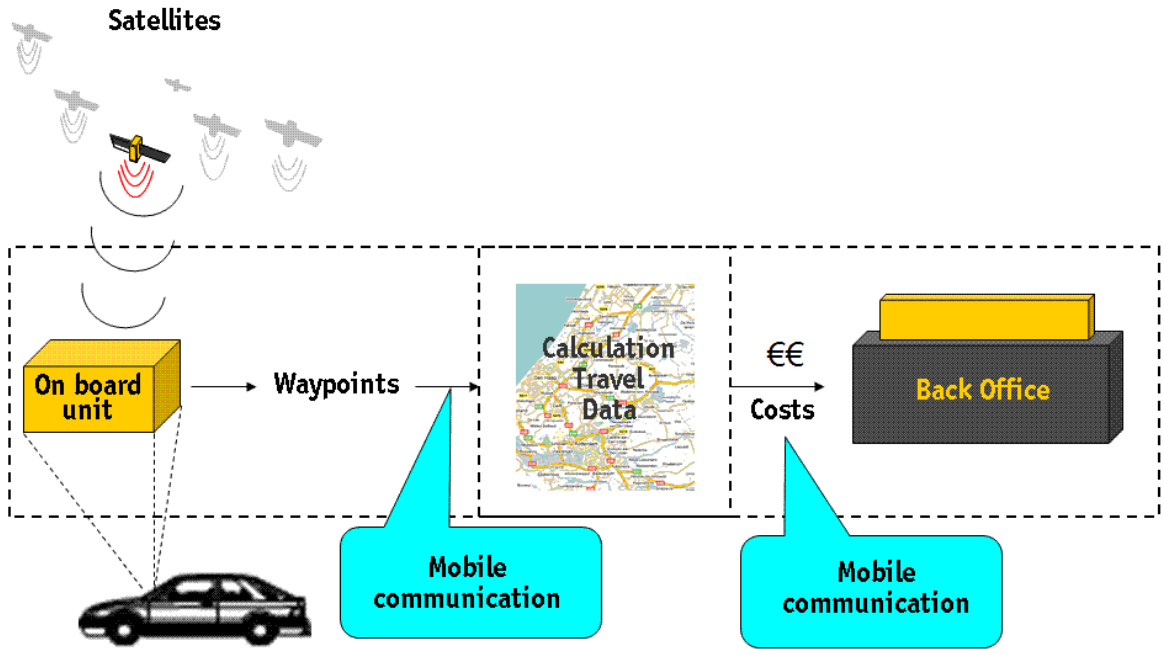

Image 1 (Source: Logica)

The present government wants to start using the system of Kilometerprijs for trucks in 2011. In the year 2016 the system should be used for all vehicles using Dutch roads.

At the moment of writing of this study it was not known which technology is going to be used for the system of Kilometerprijs. The chance however is quite high that on board units (OBUs) will be placed in vehicles. This unit, a small computer, will be used for calculating the price of using the roads. The OBU communicates with other equipment to be able to send the owner of a vehicle an invoice for road use. Depending on the content of this communication more or less privacy issues are at stake, which will be discussed below.

[168] Letter hearing kilometerprijs 31 January 2008, CBP (<www.cbpweb.nl> and search using keyword *kilometerprijs*).

6.7.4 Legal aspects of Kilometerprijs

6.7.4.1 System of payment and interoperability

Except privacy at least two other legal issues play a role in the system which should make it possible to a price per kilometer driven. The first one is related to organizational and executive aspects of Kilometerprijs such as the legal qualification of the payment system used for Kilometerprijs: price, retribution (dues/charges), levy or tax. The second one has it´s origin in Brussels and deals with the interoperability of the system.[169] Below, a short description is given of how those issues are being dealt with in The Netherlands. Next, the privacy issues related to Kilometerprijs will be described.

6.7.4.2 Organisation

The Dutch Ministry of Transport, Public Works and Water Management has done a study to the legal design of road pricing.[170] This is a comparative study in which legal aspects of pricing of various countries is discussed: Germany, Switzerland, Norway, Sweden, Austria, France, Italy, United Kingdom. In the conclusions is, amongst others, stated that a legal system should not have the illusion to be able to set rules for road pricing for a longer period of time. The pricing systems being investigated all had the adage *working by doing*. During testing and developing sometimes chaos arose from an unexpected corner, leading to the conclusion that the legal system could not do much more than facilitate the development of the systems to a certain extent.

As far as legislation is concerned in all countries being investigated is chosen for basic legislation indicating the framework of the road pricing system. By contract or delegated legislation practical issues of the road pricing system are being dealt with. Advantage of this setup is flexibility. If practical issues change, then it is not necessary to change primary legislation.

The researchers have done several suggestions for Dutch legislation for road pricing. Amongst others, they have advised not to turn into detail in primary legislation. They also said not to mention technical demands in primary legislation. That would lead to inevitable amendments as other technologies are being introduced.

As far as the legal qualification of the pricing instrument is concerned the researchers stated that comparison was hard because of the differences in national legislation. The differences became more clear looking at allocation. A choice for *tax* suggests a relation with general means, while a *levy* offers possibilities for a specific allocation of the money.

The present government has chosen for a levy and the money collected will be spend on the infrastructure. One prefers a levy to tax because the level of support in society is thought to be higher if there is a direct relationship exists between the proceeds of Kilometerprijs and expenditures for infrastructure. Having chosen for a levy there are also more possibilities to mobilize private parties in the execution of the road pricing system.

---

[169] Directive 2004/52/EC on the interoperability of electronic road toll systems in the Community, OJ L 166, 30.4.2004, p. 124–143.

[170] Juridische vormgeving beprijzing in het buitenland (in Dutch), Ministry of Transport, Public Works and Water Management, 2007 (<www.verkeerenwaterstaat.nl>, click *Mobiliteit en bereikbaarheid*, next click *Anders Betalen voor Mobiliteit*, next click *De kilometerprijs* in the left margin, next click *Vooronderzoek* and see the list of publications.

6.7.4.3 Interoperability

Directive 2004/52/EC on the interoperability of electronic road toll systems lays down the conditions necessary to ensure the interoperability of electronic road toll systems in the Community. It applies to the electronic collection of all types of road fees, on the entire Community road network, urban and interurban, motorways, major and minor roads, and various structures such as tunnels, bridges and ferries.

The Netherlands as other member states need to fulfill the requirements of the interoperability directive. This means that vehicles with European electronic toll service (EETS)-compliant equipment distributed by other (foreign) parties, should be able to participate in the Dutch road pricing system without having to take extra measures.

In reverse The Netherlands also should take care of the fact that Dutch motorists can be provided with EETS-compliant equipment and en supplementary services.

To fulfill the EETS requirements the system of Kilometerprijs should use at least one of the following techniques:

• location determination with navigation (global positioning system (GPS) or Galileo);

• mobile communication according to global system for mobile communications (GSM)-general packet radio service (GPRS);

• dedicated short-range communications (DSRC) microwave technology on frequency 5.8 GHz.

The reason for those requirements is that new electronic toll systems should be suitable for future European electronic toll services. The technology used may also be suitable for other systems as long as that does not lead to an extra burden for users or discrimination.

For heavy goods vehicles other directives are applicable. A system of kilometerprijs for road haulage should comply with directive 2006/38/EC amending directive 1999/62/EC on the charging of heavy goods vehicles for the use of certain infrastructures. Those are European rules trying to safeguard a level playing field for transport of goods. Amongst other, the rules set a maximum for tariffs related to the costs of infrastructure.

6.7.4.4 The right to be left alone and Kilometerprijs

The fact that at a certain moment in the near future every vehicle might have an on board unit (OBU) does not have to have consequences for privacy, for the right to be left alone. This will be different when the OBU makes it possible to receive messages while driving related to road use. That OBUs will be provided with a feature to receive messages is not unthinkable, because in The Netherlands the option is being discussed to keep the costs of OBUs as low as possible by creating the possibility for parties to provide value added services via the OBU. This could result in commercial parties offering services to motorists when using roads.

Off course those services can be of value, but the offering of services should only be allowed if the user of the car has given his approval; opt-in. It needs to be avoided that commercial parties spam civilians while driving. It not only invades privacy, it might also cause dangerous situations in traffic.

Already existing anti-spam rules such as article 11.7 of the Dutch Telecommunications Act forbid spamming and there is no reason for those rules not to be applicable in cars.[171] So also in a car equipped with an OBU one has a right to be left alone.

The use of an OBU for road pricing makes it possible to follow vehicles around the clock. Developing Kilometerprijs one needs to be aware of those options. In this framework suggestions are made to let an independent trusted third party manage the satellite system which makes it possible to follow cars. If certain data are wanted by for example the police, one needs to do a well motivated request to enforce the trusted third party to pass through location data of a vehicle.

Another privacy issue comes to the fore in the employer – employee relation. During working hours one does not enjoy the same privileges as outside those hours. The employment relationship brings along certain limitations of the fundamental rights of employees. Next to the enjoyment of receiving of wages stands the obligation of doing work under the authority of an employer according his instructions. As a result the employee is limited in his freedom of movement and his freedom of speech. The same is true for his right of privacy. Entering the working place an employee gives up parts of his claim for respect of privacy protection.[172]

So the employer is allowed to control the acting of personnel. However, the employer needs to set (control) goals beforehand and needs to inform the employees why he considers control important. Also the control measures taken must be in proportional relationship with the employees´ interest. And limiting measures are always coupled with the weighing of interests. So there are limitations to the power of control of the employer and the most important ones are formed by possible breach of privacy made by controlling employees.[173]

All this is also true for employees not working on the same location every day, for employees moving through traffic from one place to the other. So if drivers are being followed by their employee via Kilometerprijs or via another - private - system employers need to communicate this.

In The Netherlands the Works Council Act can also play a role in this field. Article 27 of this act says – amongst others – that an employer needs consent of the works council for decisions related to the execution and protection of personal data of employees. The same is true for provisions aimed at controlling presence, behavior, or performance of employees.

6.7.4.5 Informational privacy and Kilometerprijs

It is clear personal data are at stake in the system of Kilometerprijs. Based on kilometers driven the price is being calculated and an invoice is sent to the owner of the vehicle. Data of an identifiable or identified person are being processed, and as a result the Dutch Personal data protection act is applicable.

What plays an additional role is the fact where, what is being calculated. Are the travel data – next to the data to identify the owner of the vehicle - being sent from the on board unit to a

---

[171] The anti spam rules are based on directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201 , 31/07/2002 P. 0037 – 0047.

[172] Als de telefoon wordt opgenomen. Regels voor het registreren, meeluisteren en opnemen van telefoongesprekken, Registratiekamer, november 1996. Available on the website of the Dutch Data Protection Registrar, <www.cbpweb.nl/downloads_rapporten/rap_1996_telefoongesprekken_opnemen.pdf>.

[173] See on this issue also: F. Gilbert, No place to hide? Compliance and Contractual Issues in the Use of Location-Aware Technologies, Journal of Internet Law, Vol. 11, No. 2, 2007.

computer centre where those data are stored and processed for invoicing? Or will the travel data and price be calculated in the on board unit itself after which only the price and the necessary data for invoicing are being sent to an administrative (computer) centre for further processing.

Which system is being chosen is not of importance, personal data are at stake. A choice however has consequences for the availability and security of the data. Price and address data reveal less of ones personal behaviour than price, address, *and* travel data. So if a third party stores price and address data only and for example law enforcers do a request for data, they will not be able to back track where a vehicle went to during what period. Same is true if as a result of security leaks data become available to unauthorized persons. It is no surprise that the Dutch Data Protection Authority prefers the price being calculated in the on board unit itself.[174]

Strongly related to the system chosen for processing and storing data are the issues of data retention.

Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks has not been implemented in Dutch rules yet.[175] However, the proposal for an act has been sent to the Senate for approval, so new rules for data retention will be in force soon, which is about time because the Member States should have brought into force the laws, regulations and administrative provisions necessary to comply with this directive no later than 15 September 2007.

Question is, are the data retention directive and thus the new Dutch rules on the retaining of data applicable on the data kept for Kilometerprijs? Directive 2006/24/EC sets obligations for providers of publicly available electronic communications services or of public communications networks. One might consider the network for Kilometerprijs not te be a public one. It is a closed circuit not being used by other providers. On the other hand if Kilomterprijs is going to use the European satellite system Galileo and standards as gsm/gprs it might just as well be considered a public communications service using a public communications network. In that case, the data retention rules are applicable, meaning for The Netherlands that data processed or generated by providers should be retained for 1 year (the period chosen by the Dutch government) for Kilometerprijs, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime.

On the other hand, if one reads article 6 of the directive on the categories of data to be retained, one could conclude again that the directive and thus the Dutch rules on data retention are not applicable because the categories of data mentioned in the article can not be linked to the data generated and processed using the system of Kilometerprijs. The directive mentions mobile and fixed telephony next to Internet access, Internet e-mail and Internet telephony.

---

[174] Brief hoorzitting kilometerprijs 31 januari 2008, CBP (<www.cbpweb.nl> en zoek op trefwoord *kilometerprijs*).

[175] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105, 13.4.2006, p. 54–63.

Although the data retention rules might not be applicable, off course the data processed for Kilometerprijs by providers will be retained, if only for administrative purposes. But of what use are those data?

The databases of providers of Kilometerprijs become interesting if travel data are stored as well. But as soon as travel data are stored and processed for invoicing there might be no more need to retain those data. However, in case an owner of a vehicle questions an invoice those travel data are required to verify the price, so they probably need to be retained as well. At least for a certain period of time during which a road user can object an invoice. See for example the Swedish toll system (chapter 6.4) where data are deleted 28 days after payment.

So from a law enforcers point of view travel data should be stored in the databases of providers related to Kilometerprijs, and it might not even be necessary for the data retention rules to be applicable because the travel data are kept for administrative purposes anyway. This would result in possibilities for law enforcers to do a request for travel data under certain circumstances.

6.7.5 Conclusion

After years of discussion in The Netherlands the government has decided to choose for a road pricing system which covers the whole country: Kilometerprijs. This system will be introduced for heavy vehicles first, and must be used country-wide for every vehicle in 2016. Apart from legal aspects related to the organisation and taxation of Kilometerprijs privacy issues play a role. Those issues play a role related to the storage of data, travel data in particular. If those data are stored in an on board unit the chance on privacy infringement is less likely. Therefore this is what the Dutch Data Commissioner prefers. After all, if only the price for using the road is sent from the on board unit to a third a party for invoicing, this party or any other party will not be able find out where at what time a vehicle has been.

Privacy can also a play a role when the idea of the Dutch government to allow service providers to offer (commercial) services for on board units will be approved. In that case, however, it must be the user of the vehicle who should be able to decide whether or not he wants to be left alone.

7 Conclusions

This study gives an overview of traffic monitoring systems in use or being developed in four European countries: Belgium, Germany, Sweden, The Netherlands. Despite the fact that only four countries is being looked at the study shows that there is a variety of systems. These systems use a variety of technologies.

Despite this variety, what has become clear is that traffic monitoring systems (TMS) influence how information available of vehicles moving in public spaces is gathered, processed and stored. On the one hand, the efficiency and safety of traffic (monitoring) can justify new information flows but on the other hand, norms of appropriateness and distribution should be respected as well. How can we improve efficiency and safe driving without violating norms of appropriateness and distribution?

In order to do so Hildebrand en Soenens have given a non-exhaustive overview of some of the normative questions related to traffic monitoring. They have chosen a broad perspective, using the three principles of Roussos, Peterson et al., locality, reciprocity and understanding. This should help to provide a better understanding of how normative issues in this field can be addressed.

What they have demonstrated is that answering normative questions on Traffic Monitoring Systems cannot be a straightforward exercise. It depends on a context-specific evaluation of the criteria of locality (including Nissenbaum's notion of contextual integrity), reciprocity (minimal information asymmetry) and understanding (HMI). They also stress that that normative challenges of TMSs should be made explicit (and dealt with) as much as possible in the designer phase already.

Hildebrand and Soenens have explored normative questions in the domain of traffic monitoring systems that, amongst others, create a tension between the purpose specific use of information flows in traffic monitoring systems and secondary use of (personal) data by third parties, and between privacy of citizens and the need for the transparency of their behaviours.

Those tensions have been noticed by the researchers while doing the case studies in the various countries. Therefore, special attention is paid by Custers in his chapters on function creep and privacy.

The traffic monitoring systems described can be used for various purposes easily. The more advanced the system, the more possible purposes. However, if governments want civilians to accept and use the systems transparency is required, especially where the goal of the system is concerned. Using traffic monitoring systems for other means, function creep, does rise several questions. A very important one which almost always is being asked, no matter what type of monitoring system is being used, is related to privacy. But also when traffic monitoring systems are used for the goals they are developed for, privacy issues play a role.

This should not mean that traffic monitoring should not take place. It does mean, however, that privacy issues need to be included in the discussion on choosing or introducing suitable traffic monitoring systems. Already in the design phase as Hildebrand and Soenens have suggested.

From privacy perspective, systems that process data immediately and do not store them are the most desirable. The data should be stored for as short a time as possible and should not be used for other purposes than the purpose for which they were originally intended. Large

central databases are undesirable from a privacy perspective and may also cause maintenance problems.

However, other interests may be of more importance than privacy. When measures that may infringe privacy are considered, it is recommended that the following principles are taken into account:[176]

- Efficacy: when a particular measure does not contribute to the interest that is more important than privacy, then infringing the privacy is not necessary.
- Subsidiarity: when the interest that is more important than privacy may be achieved in another way, then choose the alternative that infringes privacy least.
- Additional measures: when a particular privacy infringement is considered necessary, take additional measures that limit or compensate the infringement as much as possible.

Although these measures appear to be rather common sense, it is important to note that they are rarely used in practice. Privacy is an interest that should be balanced against other interests. It is often wrongfully regarded as a hindrance for achieving practical results. By taking privacy issues into account in the early stages, serious problems may be prevented in later stages. This renders privacy not so much a hindrance that should be overcome, but a crucial part in balancing interests and creating broad support for decisions. One has to bear in mind that our privacy in public is at stake here. Especially, if advanced systems like the Dutch Kilometerprijs will be introduced and used Europe-wide.

Whether or not the latter will occur remains to be seen. Not in the near future, we tend to conclude. Although the European Commission has made an interoperability directive[177] the variety of systems and technologies used for traffic monitoring systems, as shown in this study, will make interoperability between various European TMSs utopian, or at least futuristic. Unless the automotive industries in cooperation with the ICT industries soon sets European standards for traffic monitoring.

For now, it seems that the development of traffic monitoring systems will be a national issue for the various member-states. Traffic will be monitored in specific areas as in London and Stockholm, or maybe even national as in The Netherlands, but for Europeans crossing borders and using roads in other member-states other solutions might be thought of to be interoperable, like the Swiss paper vignet. After all, freedom of movement should not be hindered by traffic monitoring systems.

Because of the fact interoperable (national and European-wide) traffic monitoring systems are not widely in use yet, more research should be done to privacy issues of those systems as soon as possible. After all, those systems might cause a enormous (national and trans-European) flow of vehicle data and storage thereof which might lead to abuse of those data. This reseach should result in recommendations for the development traffic monitoring systems as privacy-

[176] Vedder, A., et al. (2007) *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, The Hague: Rathenau Instituut/TILT 2007.
[177] Directive 2004/52/EC on the interoperability of electronic road toll systems in the Community, OJ L 166, 30.4.2004, p. 124–143.

friendly as possible. Systems which are designed in such a way that privacy infringements are not likely to occur.

Possibilities should be investigated for the design of monitoring and payment systems which *verify* vehicles moving on road systems and as little as possible *identify* the owners of vehicles.

8 Bibliography

Arzt, C. (2006). Video- und Mautkontrollen – Autofahrer unter Generalverdacht.

Almer, D., Spångberg, J., Alpen, F., et al, SCTP System Requirement Specification 9.0 (2).

Ateniese, G., J. Camenisch, B. de Medeiros. Untraceable RFID Tags via Insubvertible Encryption. Proceedings of the 12th ACM Conference on Computer and Communication Security (CCS), pp 92-101, ACM Press, 2005.

Bailey, D., A. Juels, P. Syverson. High-Power Proxies for Enhancing RFID Privacy and Utility. In G. Danezis, D. Martin (eds), Proceedings of Privacy Enhancing Technologies (PET), 2005.

Bosma, H. et al. (2007) Data voor Daadkracht; gegevensbestanden voor veiligheid: observaties en analyse, Rapport van de adviescommissie Informatiestromen Veiligheid, april 2007.

Bygrave, L.A. (2002) Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002.

Carey, P., E-Privacy and Online Data Protection, Butterworths, 2002.

Cervero, R. (1998). Chapter 6/The Master Planned Transit Metropolis: Singapore, The Transit Metropolis, Island Press, Washington, D.C.

Crispo, B, M. Rieback, A. Tanenbaum. RFID Guardian: A Batterypowered Mobile Device for RFID Privacy Management. In C. Boyd, J. M. Gonzáles Nieto (eds), Proceedings of the Australasian Conference on Information Security and Privacy (ACISP), Lecture Notes in Computer Science volume 3574, pp. 184-194, Springer-Verlag, 2005.

Custers, B.H.M. (2004) The Power of Knowledge, Tilburg: Wolf Legal Publishers.

Data Protection Working Party (2004). Opinion on the Processing of Personal Data by means of Video Surveillance, WP89.

Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data, WP136.

Dötzer, F. (2005). Privacy Issues in Vehicular Ad Hoc Networks. Workshop on Privacy Enhancing Technologies. Dubrovnik, available at: <www13.informatik.tu-muenchen.de/personen/doetzer/publications/Doetzer-05-PrivacyIssuesVANETs.pdf>.

El Faouzi, N.-E. (2006). Baysian and Evidential Approaches for Traffic Data Fusion: Methodological Issues and Case Study. 85th Transportation Research Board Annual Meeting January 22-26, 2006. Washington, D.C.

Federal Office for Information Security. Security Aspects and Prospective Applications of RFID Systems, <www.bsi.de/fachthem/rfid/RIKCHA_en.htm>.

Fox, R., (2001). "Someone to Watch Over Use: Back to the Panopticon", Criminology and Criminal Justice, 1: 251-276.

Gilbert, F. (2007). No place to hide? Compliance and Contractual Issues in the Use of Location-Aware Technologies, Journal of Internet Law, Vol. 11, No. 2.

Gutwirth, S. and P. De Hert (2005). Privacy and Data Protection in a Democratic Constitutional State. Profiling: Implications for Democracy and Rule of Law, FIDIS deliverable 7.4. M. Hildebrandt and S. Gutwirth. Brussels, available at <www.fidis-project.eu>.

Harmon, T., J. Marca, et al. (2006). Design, Implementation, and Test of a Wireless Peer-to-Peer Network for Roadway Incident Exchange. Proceedings of the 9th International Conference on Applications of Advanced Technology in Transportation, Irvine, University of Carlifornia.

Harvey, J. (1990) Stereotypes and Group-claims; epistemological and moral issues, and their implications for multi-culturalism in education, Journal of Philosophy of Education, Vol. 24, No. 1, p. 39-50.

Hildebrandt, M. (2008). "Distributed agency and legal responsibility: some implications of autonomic computing." Techné: Journal of the Society for Philosophy and Technology.

Inter-Environement Bruxelles, Bruxelles et le péage urbain : une solution proposée pour 2015, available online at (in French): <www.ieb.be/article/843/>.

Jiang, X. (2002). Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social. Privacy Workshop September 29, 2002, University of California, Berkeley. Berkeley, available at: <guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/jiang-privacyworkshop.pdf>.

Juels, A., Minimalist Cryptography for Low-Cost RFID Tags. International Conference of Security in Communication Networks (SCN), 2004.

Juels, A., RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications 24(2):381-394, 2006. An earlier version is available from <www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf>.

Juels, A., R. Pappu. Squealing Euros : Privacy Protection in RFID-Enabled Banknotes. Financial Cryptography (FC), 2003.

Katwijk, R. van, Koningsbruggen, P. van (2002). “Coordination of traffic management instruments using agent technology”, Transportaion Reseach Part C, 10: 455-471.

Kempen, J. van (2007) Catch me if you can! A study on identity fraud in The Netherlands, Master Thesis, Eindhoven University of Technology, Eindhoven, The Netherlands.

Kleinau, K., Drittes Auto-Kennzeichen schreckt vor Autodiebstahl ab. Innovations-Report, September 17, 2002, <www.innovations-report.de/html/berichte/informationstechnologie/bericht-12938.html>.

Kuner, C., European Data Privacy Law and Online Business, Oxford University Press, 2003.

Latour, B. (1987). Science in Action: How to Follow Scientists and Engineers Through Society. Cambridge, MA, Harvard University Press

Lisken, H., and Denninger, E. (2007) Handbuch des Polizeirechts.

Longstaff, T.A., et al. (2002) Are we forgetting the risk of COTS Products in Wireless Communications?, Risk Analysis, Vol 22, No. 1, 2002.

Ministerie van Verkeer en Waterstaat (2007). Juridische vormgeving beprijzing in het buitenland.

Müller, C. and D. Boos (2004). "Zurich Main Railway Station: A Typology of Public CCTV Systems." Surveillance & Society 2 (2/3): 161-176

Nissenbaum, H. (2004). "Privacy as Contextual Integrity." Washington Law Review 79: 101-140

Privacy Commission (1999). Opinion of 34/1999 relative to images processing carried out via video surveillance systems.

Privacy Commission (2006). Opinion 42/2006 on the law proposal creating an authentic source of vehicles' data.

Registratiekamer (1996). Regels voor het registreren, meeluisteren en opnemen van telefoongesprekken.

Roussos, G., D. Peterson, et al. (2003). "Mobile Identity Management: An Enacted View." International Journal of Electronic Commerce 8 (1): 81-100
Almer, D., Spångberg, J., Alpen, F., et al, SCTP System Requirement Specification 9.0 (2).

Royer, D., et al. (2008). Study on Mobile Identities for Transport Monitoring, FIDIS report.

Vedder, A. et al. (2007) *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Rathenau Instituut/TILT 2007.

Wessel, R., Bermuda's RFID Vehicle Registration System Could Save $2 Million/year. RFID Journal, May 18, 2007, <www.rfidjournal.com/article/view/3321/>.

Zimbuschka, J., L. Fritsch, M. Radmacher, T. Scherner, K. Rannenberg. Enabling Privacy of Real-Life LBS. Proceedings of the 22nd IFIP TC-11 International Information Security Conference IFIP Sec 2007, IFIP International Federation for Information Processing Series Vol. 232, pp. 325-336, Springer-Verlag, 2007.

Zimbuschka, J., L. Fritsch, M. Radmacher, T. Scherner, K. Rannenberg. Privacy-Friendly LBS: A Prototype-Supported Case Study. Proceedings of the 13th Americas Conference on Information Systems, 2007.

9 Abbreviations

ABMG	-	Autobahnmautgesetz
AmI	-	Ambient Intelligence
ANPR	-	Automatic Number Plate Recognition
ASCII	-	American Standard Code for Information Interchange
BAG	-	Bundesamt für Güterverkehr
BbgPolG	-	Brandenburgisches Polizeigesetz
BPA	-	Belgian Privacy Act
BremPolG	-	Bremisches Polizeigesetz
BVerfG	-	Bundesverfassungsgericht
CBP	-	College bescherming persoonsgegevens
CCTV	-	Closed Circuit Television
CDMA	-	Code Division Multiple Access
COTS	-	Commercial off-the-self
DSRC	-	Dedicated Short Range Communications
ECA	-	Electronic Communications Act
ECHR	-	European Convention on Human Rights
EETS	-	European Electronic Toll Service
FCD	-	Floating Car Data
GmbH	-	Gesellschaft mit beschränkter Haftung
GPRS	-	General Packet Radio Service
GSM	-	Global System for Mobile communications
HF	-	High Frequency
HmbDVPolG	-	Gesetz über die Datenverarbeitung der Polizei Hamburg
HMI	-	Human Machine Interface
HOT	-	High-Occupancy Toll
HSOG	-	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
IBBT	-	Institute for Broadband Technology
ILTAG	-	Intelligent License Tag
ITS	-	Intelligent Transportation System
LF	-	Low Frequency
LVwG	-	Landesverwaltungsgesetz
M2M	-	Machine-to-Machine

MautHV	-	Mauthöheverordnung
MautStrAusdehnV	-	Mautstreckenausdehnungsverordnung
Nds. SOG Ordnung	-	Niedersächsisches Gesetz über die öffentliche Sicherheit und
NextGenITS	-	Next Generation of Intelligent Transport Systems for Belgium
OBE	-	On Board Equipment also refered to as On Board Unit (OBU)
OBU	-	On Board Unit also refered to as On Board Equipment (OBE)
OCR	-	Optical Character Recognition
P2P	-	Peer-to-Peer
PAG	-	Polizeiaufgabengesetz
POG	-	Polizei- und Ordnungsbehördengesetz
PIN	-	Personal Identification Number
RFID	-	Radio Frequency Identification
RTMS	-	Remote Traffic Microwave Sensor
SIS	-	Schengen Information System
SOG MV Mecklenburg-Vorpommern	-	Gesetz über die öffentliche Sicherheit und Ordnung in
SPolG	-	Saarländisches Polizeigesetz
SSL	-	Secure Sockets Layer
TMS	-	Traffic Monitoring System
TPM	-	Trusted Platform Module
UHF	-	Ultra High Frequency
UMTS	-	Universal Mobile Telecommunications System
VANET	-	Vehicular Ad Hoc Network
VAT	-	Value Added Tax
VICATS	-	Video Content Analysis For Automated Traffic Surveillance
VSC	-	Vehicle Safety Communication
ZFZR	-	Zentrales Fahrzeugregister