FIDIS

Future of Identity in the Information Society

Title:	"D11.5: The legal framework for location-based services in Europe"
Author:	WP11
Editors:	Colette Cuijpers (Tilburg University, The Netherlands), Arnold Roosendaal (Tilburg University, The Netherlands) Bert-Jaap Koops (Tilburg University, The Netherlands)
Reviewers:	Mark Gasson (University of Reading, UK) Wim Schreurs (Free University Brussels, Belgium)
Identifier:	D11.5
Type:	Report
Version:	1.0
Date:	Tuesday, 12 June 2007
Status:	[Final]
Class:	[Public]
File:	fidis-WP11-del11.5-legal_framework_for_LBS.doc

Summary

This deliverable investigates legal certainty and privacy protection with regard to Location Based Services (LBS). The main question is: Which legal data-protection framework applies when providers of location-based services (LBS), public authorities and private parties like employers process location data generated in positioning systems? General descriptions provide a background to understanding the techniques used in LBS and the applicability of the relevant European legal framework. The practical implications of the European legal framework for the national level are described in four country reports: Belgium, France, Germany, and the Netherlands.

The main conclusion is that the applicability of legal provisions to varying forms of LBS and of processing location data is unclear. This is due to the very complex legal framework, which uses overlapping and not clear-cut definitions in three European Directives and in national implementations. The resulting legal uncertainty for European citizens and for providers of LBS and the enhanced privacy risks for citizens and employers should be overcome by a reassessment of the European legal framework.

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

Copyright Notice

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. Centre technique de la Gendarmerie Nationale (CTGN)	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	10.12.06	• Initial format for the deliverable (Colette Cuijpers, Arnold Roosendaal)
0.2	23.12.06	• Initial format general legal framework (Colette Cuijpers, Arnold Roosendaal)
0.3	02.01.07	• Country report Belgium and France (Fanny Coudert, Eleni Kosta)
0.4	24.01.07	• Draft technical chapter (Martin Meints, Denis Royer)
0.5	08.03.07	• Country report Germany (Maren Raguse)
0.6	19.03.07	• General legal framework (Colette Cuijpers, Bert-Jaap Koops, Arnold Roosendaal)
0.7	22.03.07	• Country report Netherlands (Colette Cuijpers, Bert-Jaap Koops, Arnold Roosendaal)
0.8	26.03.07	• Update technical chapter (Martin Meints, Denis Royer)
0.9	16.04.07	• Final version for internal review (Colette Cuijpers, Arnold Roosendaal)
1.0	12.06.07	• Processing internal reviews. Final editing for final version (Bert-Jaap Koops)

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)*
1 Executive Summary	Arnold Roosendaal, Bert-Jaap Koops (TILT)
2 Introduction	Colette Cuijpers (TILT), Arnold Roosendaal (TILT)
3 Location Information from a Technical Perspective	Martin Meints (ICPP), Denis Royer (JWG)
4 Location Information from a European Legal Perspective	Colette Cuijpers (TILT), Arnold Roosendaal (TILT), Bert-Jaap Koops (TILT)
5 Location Information from a Belgian Perspective	Fanny Coudert (ICRI/KU Leuven), Eleni Kosta (ICRI/KU Leuven)
6 Location Information from a French Perspective	Fanny Coudert (ICRI/KU Leuven)
7 Location Information from a German Perspective	Maren Raguse (ICPP)
8 Location Information from a Dutch Perspective	Colette Cuijpers (TILT), Bert-Jaap Koops (TILT), Arnold Roosendaal (TILT)
9 Conclusions	Colette Cuijpers, Bert-Jaap Koops (TILT)
10 References	Arnold Roosendaal (TILT)
11 Abbreviations & Glossary	Arnold Roosendaal (TILT)

Table of Contents

1 Executive Summary

Mobile communications and services are among the most rapidly expanding fields of today's technology. Wireless systems and unique identification of communication devices, combined with location data, enable providers to deliver Location Based Services (LBS). These services can vary from weather forecasts on mobile phones to automatic route planning. LBS will soon become an integral part of daily life.

An important factor for developing and operating LBS is the legal framework. This should serve at least two purposes: the development of LBS should be fostered by legal certainty for providers and consumers, and the privacy of citizens, consumers, and employees should be adequately protected now that people's movements can be monitored pervasively and accurately. With this in mind, this report aims at answering the following question:

> Which legal data-protection framework applies when providers of location-based services (LBS), public authorities and private parties like employers process location data generated in positioning systems?

In order to answer this question, this report describes technologies facilitating positioning of people, such as mobile communications, GPS, RFID, and WiFi. It describes the European legal data-protection framework for Location Based Services and provides an overview of LBS provisioning in relation to the national legal frameworks in Belgium, France, Germany, and the Netherlands. These country chapters also give examples of existing LBS applications, illustrating that problems with legal certainty in different legal regimes are far from theoretical.

The most relevant element in the legal framework for LBS is the data-protection regime for location data. Depending on the kind of data and circumstances, location data can be personal data and/or telecommunications traffic data. The European legal regime for these data can be found in three European Directives, on Data Protection, Privacy and Electronic Communications, and Data Retention.

The legal framework for processing location data generated in positioning systems is very complex indeed. Given the wide variety of positioning systems based on diverging technologies, and the three Directives that use partly overlapping definitions of personal data, traffic data, and location data, it is a Herculean task to determine which legal provisions apply when LBS providers, public authorities and private parties process location data.

Apart from the vast complexity of the legal framework, problems are also caused by unclear definitions and unresolved legal questions. Major open questions are whether 'standby' location data qualify as traffic data, which LBS systems are 'publicly available' electronic communications systems, whether sensor-based (RFID, WiFi) and chip-card-based systems involve electronic communications, and how consent should be given in the context of location systems. As a result, the legal certainty offered by the European legal framework is poor. The same holds for the national legal frameworks studied in this report, where similar problems occur. It is therefore recommendable that at the European level, the legal framework for processing location data be clarified and simplified.

Moreover, it is questionable whether the legal frameworks provide adequate privacy protection in the context of positioning systems. They allow much scope for public and private parties to infringe the privacy of citizens and employees through monitoring their movements. The increasing pervasiveness and accuracy of positioning devices, the recent

requirements for traffic data retention, and the rise of non-public localisation systems lead to an enhanced privacy risk that may have to off-set by new checks and balances.

In conclusion, the development of positioning systems and location-based services may offer great opportunities for Europe, provided that the legal framework is improved. A reassessment and clarification of the European legal framework for processing location data is urgently needed, both to adequately protect citizens' privacy and to foster the development of location-based services in Europe.

2 Introduction

2.1 Background

Over the past decade, we have become used to surveillance techniques surrounding us. Monitoring of personal computers by governments as well as employers or just the prying Nosy Parker, camera surveillance in public places and access control mechanisms to enter – or to prevent entering – certain places, have become common examples. Issues such as security, the fight against terrorism as well as combating fraud makes the intrusion these techniques make upon our personal lives acceptable to a certain level. Off course, some legal as well as technical boundaries are in place, but there still seems to be some truth in pessimistic views announcing the increase of the unwanted gaze. Recent technological developments take monitoring to an even higher level, in a sense new techniques make it possible to track and trace products as well as persons 24/7 on a global scale.

The processing of location data in relation to identifiable persons raises the question as to whether the existing legal framework, which should offer protection against different types of surveillance techniques, is adequate to cope with the new or intensified dilemmas that arise out of the processing of location data. In this respect the technical design of the system, including the different people involved in developing and operating the system, as well as the functionality of the system in combination with the gathering and use of the identifiable location data is of interest.

Even though the legal regime regarding the processing of personal data, as well as the processing of traffic data[1] and location data, is harmonised within the European Union, this does not guarantee the same level of protection within each Member State. The complexity of the European legal framework which is based on several overlapping European directives, the multitude of complicated definitions which are susceptible to multiple interpretations, and the margin of appreciation left to the Member States are all factors that make it interesting to view this topic from several jurisdictions.

In this study a comparison is made between Belgium, France, Germany and the Netherlands. These countries have been chosen as a group of countries with a close geographic connection, and with legal systems that are often similar but that do have differences, and which all have implemented the relevant legal European Directives in their laws. Because of the geographic connection and the common European market, the sharing of (personal) location data or telecommunications traffic data between them in LBS can easily become a practical issue. Therefore, it is of interest to take a closer look at the different national legal regimes in order to assess whether or not differences within these systems influence the protection of individuals with regard to the processing of their personal, traffic, and/or location data, and whether differences in implementation of the Directives impact upon the technical and commercial opportunities of providing LBS across these countries.

From Location Based Services already in use, it becomes clear that two specific relationships are in need of special attention because of particular challenges and problems that exist with

[1] ‚Traffic data' in this deliverable refers to electronic-communications traffic data, i.e., data about who telecommunicated with whom when, how long, and where. This term is commonly used in the telecommunications sector and the legal framework regarding electronic communications. Therefore, it does not refer to road-traffic data!

regard to the processing of location data within these relationships. One is data processing by public authorities, more specifically by law enforcement authorities, and the other is data processing by private parties, in particular by employers.

2.2 Structure and contents

Against this background, we aim at answering the following central question in this deliverable.

> Which legal data-protection framework applies when providers of location-based services (LBS), public authorities and private parties like employers process location data generated in positioning systems?

In order to answer this question, the study is divided into three parts:

I. An introduction into the technical and legal background regarding Location Based Services (Chapters 3 and 4).

II. An overview of the implementation of the European legal framework, as well as the provisioning of Location Based Services and the national legal framework in four European Member States (Chapters 5-8).

III. A conclusion regarding the central question of this deliverable (Chapter 9).

In order to be able to draw some general conclusions with regard to the central question of this study, several subquestions have been identified which have guided the authors of the individual country chapters.

1. Describe existing use of mobile ID and GPS systems generating location data. Give examples of these systems and their use in your country. And/or describe future scenarios. Take into consideration the technical specifications of these systems that can limit or condition generating and accessing location data.

2. Describe the legal framework in your country regarding generating and using location data by public authorities. Which conditions apply to requests for location data from LBS providers? Which powers exist for police to order LBS providers to preserve (‘freeze’) location data? Is there a requirement for data retention?

3. Describe the legal framework in your country regarding generating and using location data by private parties, in particular employers. Which conditions apply to requests for location data from LBS providers? Are there specific procedures how to deal with those requests? Who is / are involved in the weighing of interests, the provider, judge, others?

4. Does your legal framework offer an adequate balance regarding on the one hand the interests of (private/public) access to and use of location data and on the other hand (private/public) interests of privacy and anonymity? Do the technical specifications of the systems offer protection against invasion of privacy? If the conclusion is drawn that no adequate guarantees exist, how could (what kind of) guarantees be achieved?

Even though each and every country chapter does not explicitly address all of these questions, together with the general technical and legal chapter, they provide sufficient information to draw general conclusions with regard to the central question and the subquestions of this study. These conclusions are summed up in Chapter 9 along with some recommendations on how to clarify the complex technical and legal framework that currently exists with regard to

the processing of personal, location, and/or traffic data and the negative consequences this might have for the further development of Location Based Services.

3 Location Information from a Technical Perspective

Martin Meints (ICPP) & Denis Royer (JWG)

Location information is needed for a number of different Location Based Services (LBS). This chapter gives an overview of how location information[2] can be generated and how it can be processed. We offer various classifications and schemes of techniques and systems that can be used to determine the location of persons or objects. Other classifications are of course possible, but our overview should help the reader to understand the variety in LBS techniques and applications that are currently in use or being developed.

3.1 Generating location information

Location information can be generated using different technologies. There is a variety of technologies available today, which are used to get the position of an entity (person, object, etc.). In this document, the following classification is used:

- Satellite-based positioning systems such as the Global Positioning System (GPS) or the European Galileo system[3]
- Sensor-based systems:
  - Certain implementations of biometrics[4], such as face recognition systems used in public places (e.g. stadiums, train stations, or airports) in the context of tracking and tracing persons
  - Optical sensors allowing for identification of objects (such as license-plate scanners for vehicles)
  - Passive, infrared-based location systems (e.g. PDAs used in museums to guide visitors)
- Other wireless technologies, such as Radio Frequency Identification (RFID)[5] based systems or wireless communication systems, such as WiFi or Bluetooth
  - Using location of known objects (e.g. an RFID or Bluetooth beacon)
  - Using triangulation[6] to establish a more detailed location of a person or object
- Cell-based mobile communication networks such as GSM and UMTS[7]
  - Using location of known objects (e.g. the location of a base station)
  - Using triangulation to establish a more detailed location of a person or object (using several base stations)

---

[2] In this chapter, we use the terms ‚location information' and ‚location data' in the technical and common-language sense of information and data about the geographic location of something or someone. In the context of this report, it should be borne in mind that not all of these location data qualify as ‚location data' in the legal sense as outlined in Chapter 4, and that not all LBS systems we describe here qualify as ‚electronic communications' networks or services in the context of Directive 2002/58/EC. Cf. section 4.3.2.

[3] More at: <http://ec.europa.eu/dgs/energy_transport/galileo/index_en.htm>.

[4] Biometrics have been described and analysed in the FIDIS deliverable D3.2 “Study on PKI and Biometrics”.

[5] RFID is introduced in the FIDIS deliverable D3.7 “A structured Collection on Information and Literature on Technological and usability Aspects of Radio Frequency Identification (RFID)”.

[6] Triangulation is the process of finding coordinates and distance to a point by calculating the length of one side of a triangle, given measurements of angles and sides of the triangle formed by that point and two other known reference points.

[7] Mobile communication networks have been analysed in D11.1 “Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity”.

- Chip-card-based systems:
  - Payment systems such as credit cards and Maestro Cards used at a certain ATM
  - Personalised access cards of employees to access (certain parts of) a building.

3.2 Quality of location data

Since theses technologies differ a lot in the way they work and in their positioning accuracy, Table 1 and Figure 1 give a brief overview of these characteristics. Furthermore, some of the limitations and possibilities to disturb or manipulate positioning technologies are presented (see Table 1).

Technology	*Accuracy*	*Note*
Satellite-based positioning systems: **GPS, Galileo**	>1m-15m	• The accuracy of satellite-based systems depends on the service/technology being used. • GPS is mostly used outdoors since the signals are generally too weak to be received inside buildings. • Satellite signals can be jammed or the accuracy can be altered by the government in case of a military emergency. • Examples of systems in use: A-GPS[8], GPS.
Cell-based mobile Communication Networks: **UMTS (3G), GSM (2G)**	25m – 30km	• Most mobile network-based positioning technologies only offer a limited accuracy with regard to the positioning of the mobile device. • The accuracy depends on the size of the communication cell, the mobile device resides in. In city centres, the diameter of a cell can be approximately 300 metres, in rural areas much larger cells (diameter up to approximately 30 km) exist. Additional technologies, for example using triangulation, allow more accurate positioning. • Examples of systems in use: E-OTD[9], Cell-ID.
Other wireless Technologies: **Radio Frequency Identification (RFID), WiFi, Bluetooth**	<1m – 50m	• Theses technologies use a similar approach as cell-based systems to determine the position of an entity. • Several "base stations" are needed to perform the triangulation. However, the accuracy heavily depends on the technology and the amount of "base station" being present in the observed area ➔ mostly these technologies are used indoors.

[8] Assisted GPS (A-GPS): Based on GPS, this technology uses an assistance server to cut down the time needed to determine a location. This results in a lower power consumption on the handset, since less processing is needed.
[9] Enhanced Observed Time Difference (E-OTD): Measures the time of arrival of a base station signal on the handset. The precision of this method depends on the number of available base stations in the network (varies from 50 to 200 m).

Sensor-based Systems: **Optical sensors (infrared-based), biometrics (face recognition)**	Close proximity: >10cm – several metres	• Sensor-based systems resemble a conglomeration of different location technologies. • Their accuracy and precision depends on the technology being used – also, the technologies themselves differ a lot in the way that they work (e.g. optical systems vs. wireless systems).
Hybrid Systems	N/A	• These technologies include systems that use combinations of different positioning technologies to offer a higher positioning precision. • Example: Assisted GPS (A-GPS), combining GPS technology with external sensors (e.g. tachymeter) or cell-based positioning technologies (mobile phones, etc.).
Automated Teller Machines (ATM)	Direct contact with a ATM terminal	• A positioning is not possible on a continuous basis. However, the position of its user can be determined by the position of the terminal being used to access the card's information.

Table 1: Positioning Technologies used for Location Based Services (LBS)[10]

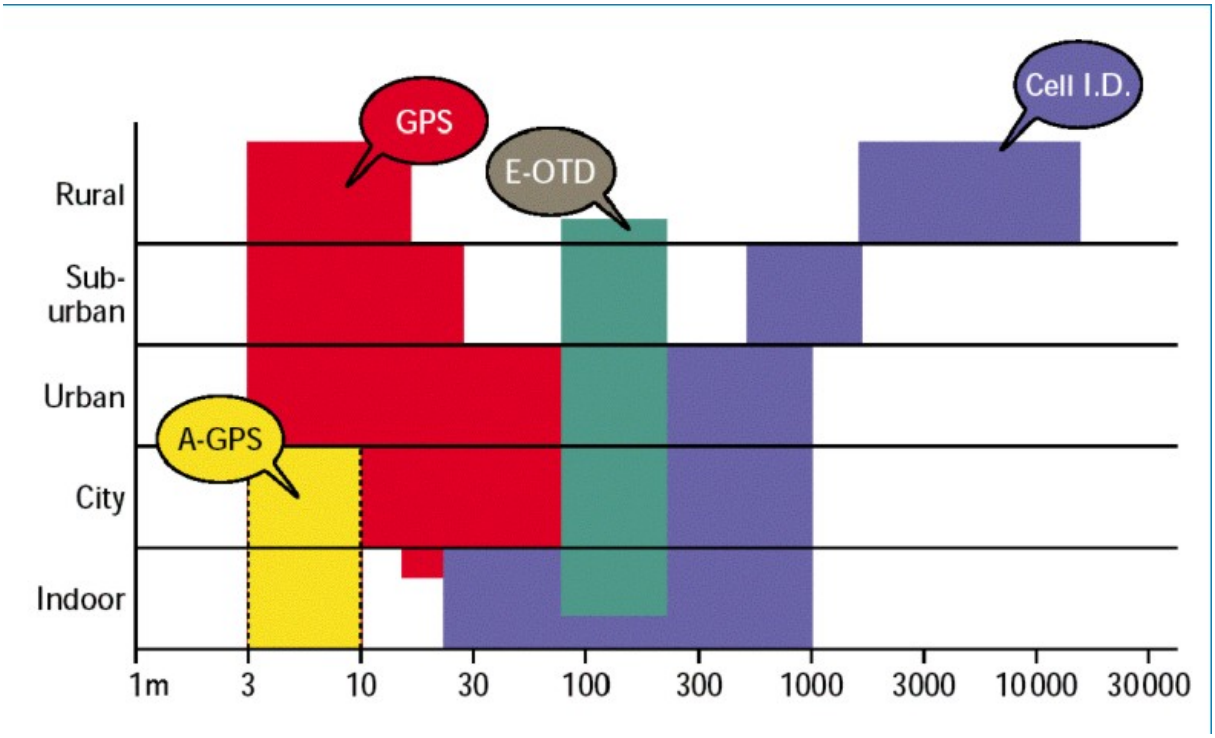

Figure 1: Location Technologies used in Cell-based communication Networks (in GSM: A-GPS, GPS, E-OTD, Cell-ID) and their Accuracy[11]

Moreover, location information typically is generated in location systems, which typically consist of two or three types of components:

[10] For more details on the technologies being presented, please refer to FIDIS deliverable "D11.2: Location Based Services" available at: <http://www.fidis.net>.
[11] Based on <http://nds2.ir.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/mlbs.pdf>.

1. One or more devices sending location information to sensors – in the case where sensors do not operate optically.
2. Sensors to receive and transfer location and time information to static or mobile backend systems.
3. Backend systems interpreting and / or using location information.

Component one and two can be combined, for example in case of optical sensors such as video surveillance cameras, face recognition systems, or license plate scanners.

3.3 Fixed and mobile sensors or objects

Location systems typically need a static and a mobile component, leading to two operational modes of location systems.

1. Static sensors and mobile devices or objects bearing or transmitting location information; in this case the location information is given by the position of the identifiable sensor and can be interpreted using, e.g., reference databases (cf. Figure 2), and
2. Mobile sensors and static objects bearing or devices transmitting location information; in this case the location information is given by the identifiable object or device. In this case reference databases can also be used.

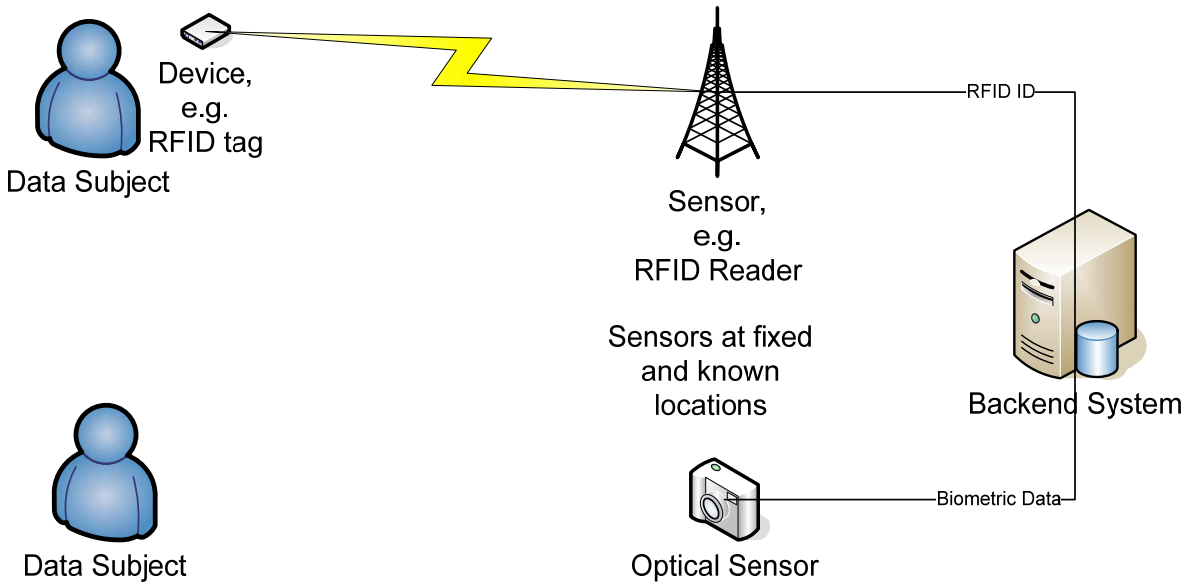

Figure 2: Schematic of a location system with static sensors at known locations

Examples for the use of static sensors are:

- Toll collection systems using RFID (e.g. Intelligent Highway Vehicle Systems in the USA) or optical sensors (e.g. TollCollect[12] in Germany)
- RFID systems using static RFID receivers in logistics, service points, electronic-detention systems etc.
- Location data generated by mobile phones in GSM cells (in this context the static GSM sender contains the sensor for the GSM cell)

[12] More at: <http://www.toll-collect.de>.

- Biometric systems, using static (optical) sensors such as video surveillance systems at a fixed location in combination with face recognition systems, finger printing systems, iris scan systems etc.
- Border control systems using ICAO-compatible Machine Readable Travel Documents (MRTDs)[13]
- Indoor positioning systems based on wireless technologies, such as WiFi or Bluetooth.
- ATMs and other paying machines where users identify themselves with a bank card.

Examples for the use of mobile sensors are:

- Use of satellite-based positioning systems such as GPS and the future European system "Galileo",
- RFID systems used, e.g., in museums (Hildebrandt, Meints 2006) and fully automated warehouses[14], where the RFID tags are fixed at certain locations and the receivers are used mobile by visitors of the museum or vehicles carrying goods around in the warehouse.

In addition, location information can be generated automatically and continuously, automatically in certain time intervals (both also used by push services) or by request (also used by pull services, see Nassary-Zadeh 2007).

3.4 Transferring location information

After the location information has been generated, it is transferred to the backend system, where it is interpreted and / or used. The transfer of location data can be done using mobile (wireless) or wired networks. The backend system can be operated at a fixed location such as a toll collection system, a tracking system for goods etc., or in a mobile way such as a navigation system in vehicles. In some cases, the results of the processing of location data are transferred to another device. Examples for this are personal LBS such as the "buddy finder services", where the location information after central processing by a service provider is transferred to the mobile phone of the customers of the service (see Figure 3 or Nassary-Zadeh 2007). In this case, three parties are involved (see Figure 3 below):

- The mobile user (customer) using the LBS.
- The mobile operator (MO) giving access to the communication network, identifying its users, and locating the users' positions. Furthermore, the MO transfers the location to the LBS provider.
- The LBS provider, providing the requested service to the mobile user.

[13] ICAO-compatible MRTDs have been described and analysed in the FIDIS deliverable D3.6 "Study on ID Documents".
[14] See for example: <http://www.directionsmag.com/press.releases/index.php?duty=Show&id=7702&trv=1>.

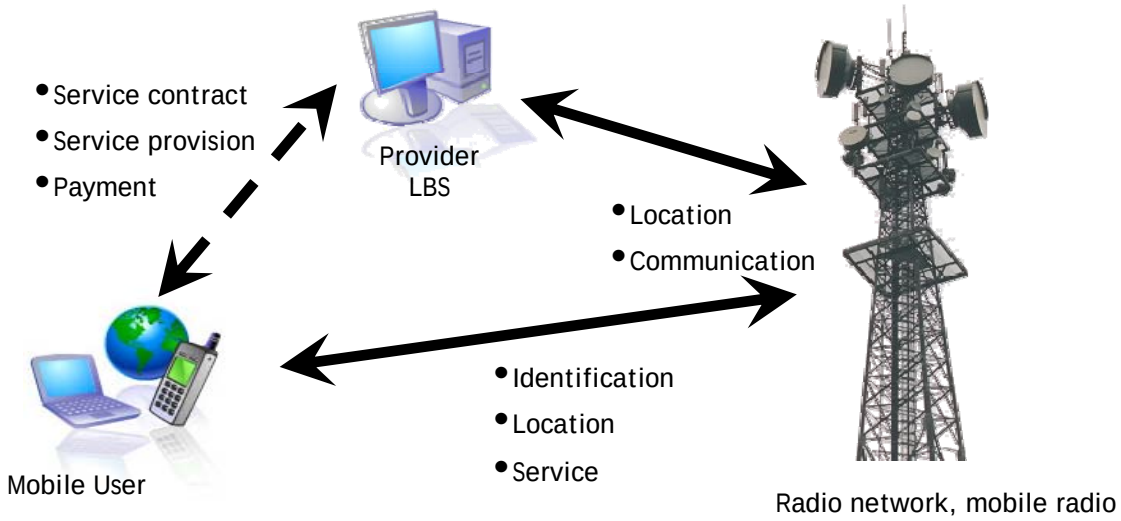

Figure 3: GSM-based LBS – The Parties Involved

3.5 The usage of location information

Location information can be used for a number of different purposes, for example:

- Tracking and tracing of goods; objectives:
  - Supply Chain Management (SCM); this includes securing and monitoring of the quality of goods when transporting them
  - Manufacturing Management (MM)
  - Fleet management in cases of logistic service providers
- Tracking of persons; objectives such as:
  - Authentication
  - Authorisation
  - Access control; this includes security checks in transactions, e.g., money transfer via ATMs, electronic foot cuffs used for electronic (home) detention, services for leisure etc.
  - Social networking, such as friend-finders and 'gaydars'
- Security, e.g., monitoring children or elder people using GPS-GSM-based tracking systems,[15] but also monitoring of money-transporting vehicles
- Emergency response and planning for rescue operations (disaster management, tagging of injure people, etc.)
- Navigation
  - On the road when driving (orientation),
  - In certain areas, e.g., cities (example: points of interest)
  - Off-road; objective also optimisation of the use of fertilisers, weed killers and insecticides in agriculture.

3.6 The link between location information and physical persons

In order to assess which legal framework applies to location data, it is important to know whether the location data are linkable to an individual person; in that case, they qualify as

[15] See for example: <http://www.wherifywireless.com/corp_home.htm>.

personal data (see section 4.2). Here, we give a rough indication of the linkability between location data and individuals for different LBS techniques; a legal assessment is more complex and often depends on concrete circumstances (see further sections 4.2 and 4.3).

In some cases there is no possible link between location information and a person, especially when location information is used in the context of objects only. One example for this is location information in the context of a fully automated warehouse. In this example location information refers to places in the warehouse and is used by machines only.

In most cases there will be a link between a device or a sensor used for LBS and a person. This link can be direct, e.g., by using purpose-specific devices (e.g. mobile emergency phones) and very stable, e.g., physical properties of the person (biometric features) or implants (both of them can not easily be changed). In many cases, however, this link is only indirect, for example in cases where a person uses an object which has an attached device that is part of the location system (e.g. a vehicle with GPS sensor, a product tagged with an RFID tag etc.). Indirect links can be fairly strong, i.e., with a reasonably high probability that the object and person are linked (e.g. a mobile phone of a consumer), but they can also be quite weak (e.g. with a company vehicle that is driven by several employees).

The following table gives an overview of the possible properties of the link between location data and a person for selected technological examples.

Technology examples	Linked to individual persons	Strength of the link
1) static sensors		
1a) RFID in logistics	Usually no link when RFID tag is removed at the end of the logistic chain	
1b) RFID implants	Always linked	Link is direct and very strong
1c) toll-collection	Usually linked for private vehicles (not for company vehicles)	Link is indirect and not strong, through car owner
1d) mobile phones	Usually linked, except in cases of certain prepaid cards	Link is indirect through phone number and reasonably strong
1e) license plate scanners	Usually linked	Link is indirect and not strong, through car owner
1f) Tracking using biometrics	Linked through biometric features	Link is direct and can be very strong, depending on the quality of the biometric system
1g) Chip-card location	Linked to location of the reader	Link is direct
2) mobile sensors		
2a) GPS for objects	Possibly linked	Link is indirect, e.g. car navigation linked to car owner
2b) GPS for persons	Usually, e.g., in route systems	Link is indirect through the GPS locator
2c) RFID sensor on persons	Usually linked	Link is indirect through the sensor
2d) RFID sensor on objects	Usually not linked	

Table 2: Examples of different types of links between location data and a physical person

3.7 Issues of control

In cases where location data is linked to a person, control of generation and processing of these data is legally relevant. Control issues can be complex, as generating and processing of location data in many cases is not done by the same organisation (or data controller). Generation of location data and/or processing may be done continuously (or online) or by requests at a certain time. In addition, the generation and processing may concern location data of the user of a location system himself (typically in cases of so-called LBS used via mobile phones) or of another person (e.g. in cases of tracking).

With respect to issues of control, no classification of LBS seems to have been published in the literature.

3.8 Security of location systems

From a legal point of view, how location data in location systems can be secured e.g. against unauthorised access, is of interest. This especially concerns location data corresponding to persons. As already described, location systems typically use IT systems at least in the backend to store and process location data. In most cases the whole location system can be classified as an IT system. Therefore internationally accepted security standards apply.

These standards can be classified in product-related and procedure or organisation-related standards. In the context of products the Common Criteria[16] (CC; ISO/IEC 15804) are established. They allow the definition and certification of e.g., so-called Security Functions (SF) a product offers. Security Functions can be e.g., encrypted storage of data, effective access control mechanisms, etc.

For the implementation and operation of IT systems typically Information Security Management Systems (ISMS) are used. Based on the results of a risk analysis, technical and organisational security measures are used in combination to reduce risks until they are acceptable for the organisation. To ensure the effectiveness and appropriateness of the selected measures in running operations of IT systems, a process based IT Security Management is used. ISO/IEC 27001 offers 'good practice' examples for ISMS. For technical security measures classifications (e.g. ISO/IEC 17799) and catalogues (e.g. the Baseline-Protection-Catalogues[17] offered by the German Federal Office for Information Security) are available.

In combination these different standards allow for an effective IT security management with respect to all steps of the life cycle of location systems: *planning*, *building* and *operations*.

Common Criteria certificates have not been applied for products in the context of location systems so far, because of a check of publicly available certificate lists of certificate bodies in the United States,[18] Canada,[19] the UK,[20] Australia,[21] and Germany.[22] ISMS have already been

[16] Download available e.g. via: <http://www.bsi.bund.de/literat/faltbl/F06CommonCriteria.htm>.
[17] See: <http://www.bsi.bund.de/gshb/deutsch/index.htm>.
[18] See: <http://www.niap-ccevs.org/cc-scheme/vpl/>.
[19] See: <http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html>.
[20] See: <http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=15>.
[21] See: <http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html>.
[22] See: <http://www.bsi.bund.de/zertifiz/zert/report.htm>.

implemented in the context of location systems, mainly in computer centres of mobile communication and location providers. One example of this is Vodafone IT Operations.[23]

3.9 Conclusion

Different kinds of technologies can be used to provide Location Based Services (LBS):

- Satellite-based positioning systems;
- Sensor-based systems;
- Other wireless technologies, such as Radio Frequency Identification (RFID) based systems or wireless communication systems, such as WiFi or Bluetooth;
- Cell-based mobile communication networks;
- Chip-card-based systems.

Since theses technologies differ a lot in the way they work, their characteristics and in their level of accuracy, they are suitable for different kinds of LBS. Furthermore, there are differences with regard to the limitations and possibilities to disturb or manipulate these positioning technologies. Also the purpose for which location data are required will influence the choice of a technology best suited to provide a certain LBS.

In LBS, location information typically is generated through location systems that usually consist of two or three types of components:

1. One or more devices sending location information to sensors in case sensors do not operate optically.
2. Sensors to receive and transfer location and time information to static or mobile backend systems.
3. Backend systems interpreting and / or using location information.

In this respect, not only differences exist with regard to the technologies used to provide LBS, but also with regard to the parties involved in the process. This means that control issues regarding the data that will be generated within these location systems can be complex, as generating and processing of these data in many cases is not done by the same organisation (or data controller). In view of these differences, it is interesting to study how LBS impact upon privacy and data protection and how the various kinds of LBS and location information relate to the legal framework for personal data, traffic data, and location data.

[23] See: <http://www.iso27001certificates.com/>.

4 Location Information from a European Legal Perspective

Colette Cuijpers, Arnold Roosendaal & Bert-Jaap Koops (TILT)

4.1 Introduction

Location Based Services (LBS) do not only function in a technical and organisational context, but also in a legal context. Whereas the previous chapter sketched the various techniques and modes used in LBS systems, this chapter will give an overview of the relevant EU legislation on the processing of location data with regard to the provision of LBS.

The relevant European legislative framework consists of several Directives that relate to the processing of personal data in general, the processing of personal data in the electronic communications sector, and provisions regarding obligations for data retention. The main difficulty with this European framework for LBS data lies with the legal definitions and qualification of different groups of data and the overlap that exists between these groups. Also the fact that the different directives are addressed to different parties and the technology-dependent applicability of the rules make the legal framework for location data a complex issue. In this chapter, we try to provide some clarity on the European legal framework, which will serve as a background to the four country reports given in the next chapters.

First, this chapter will provide an insight into the different European Directives that are applicable to location data. The starting point is the general European Directive on the processing of personal data, followed by more specific directives concerning the processing of personal data in electronic communications and the Data Retention Directive.[24] From these different directives, it becomes clear that a distinction needs to be made between personal data, traffic data, and location data. However, due to overlap, this distinction is not always easy to make as all kinds of combinations are possible, e.g., personal data can be location data as well. This leads to a complicated picture regarding the applicability of the regimes laid down in the directives with regard to the different kinds of data. This picture becomes even more complicated when assessing whether certain kinds of technologies used to process these data fit the definitions of communication services and networks as laid down in Directive 2002/58/EC. We give an elaborate description of the terminology in the relevant Directives in sections 4.2 and 4.3, with a first attempt to schematically represent the different legal regimes that apply to the various kinds of data (personal, traffic, and location data). In section 4.4, we then attempt to illustrate the applicability of the different directives to the various kinds of data and technologies, by schematically showing the different possible combinations of personal, traffic, and location data and giving tentative examples of these combinations. We hope that this first attempt to illustrate the complex legal framework can serve as a basis for future refining and extension, both theoretically and practically.

Section 4.5 discusses some further distinctions made within the European legal framework that are of relevance to the applicability of this framework as well as to its practical application. Mention is made of the difference between the processing of data within private and public relationships; the difference between subscribers and users in respect of consent; the difference between direct and indirect provision of services; and the difference between

[24] In this chapter we only consider EU-internal provision of LBS. When a controller of personal data is not established within an EU Member State, Chapter IV of Directive 95/46/EC will be applicable. See in this respect Working Party 29, *Opinion on the use of location data with a view to providing value-added services*, 2130/95/EN, WP 115, November 2005, p. 4.

direct and indirect access to certain data. The last sections address two relationships in which specific rules apply or complications exist when traffic or location data are being processed. Section 4.6 concerns the processing of traffic and location data by law enforcement, and section 4.7 addresses the processing of these data within an employment relationship.

4.2 Personal data: Directive 95/46/EC

The general framework with regard to the processing of personal data is Directive 95/46/EC[25] (hereinafter: Data Protection Directive). Whether or not this directive is applicable depends on whether there is 'processing' of 'personal data'. The definition given of processing is very broad in scope and it is fair to say that almost all handling of data, from their establishment to their destruction, can be considered processing as meant by the Data Protection Directive.[26]

Whether or not data can be considered to be personal is more difficult to establish. According to article 2 sub a) of the Data Protection Directive, personal data shall mean:

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

In this definition *identification* of a *natural person* forms the main criteria. Identification can be direct, as well as indirect. Direct identification means identification without the use of a third source. Indirect identification concerns for example identification on the basis of an identification number. In this case, a third source is necessary to link the identification number to directly identifiable factors such as a name. An identification number can be a national identification number[27], as well as other numbers, such as an employee number or an IP-address. IP-addresses allow indirect identification. IP addresses can be traced back to a computer, and through the Internet Service Provider to a subscriber. Also dynamic IP addresses can be traced back to a computer. Although the link between subscriber and user is less strong compared to e-mail addresses and phone numbers, most IP addresses can be tied to a log-in and therefore may qualify as personal data.[28]

On the basis of article 29 of Directive 95/46/EC, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established. This Party has an advisory and independent status and has given opinions on all kinds of issues related to the processing of personal data in order to clarify the existing legislation. At the moment (March 2007), the Article 29 Working Party is preparing a document with explanations on the scope of the term 'personal data', as national implementation laws show differing interpretations of this concept.[29]

---

[25] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *OJ* L 281/31, 23.11.1995.

[26] However, discussion is possible regarding the question as to whether mere transfer of data within computer networks should be viewed as processing.

[27] Kaspersen H.W.K. 2002. Data protection and e-commerce, in: Lodder A.R. & Kaspersen H.W.K. (Eds.), eDirectives: Guide to European Union Law on E-Commerce, The Hague/London/New York: Kluwer Law International 2002, pp. 119-145.

[28] Asscher, L. F. 2004. Regulating Spam: Directive 2002/58 and Beyond (May 1, 2004), p. 47. Available at SSRN: <http://ssrn.com/abstract=607183 or DOI: 10.2139/ssrn.607183>.

[29] Article 29 Data Protection Working Party, Work Programme 2006-2007, document nr. 00744/06/EN, WP 120.

4.3 Personal data in electronic communications: Directive 2002/58/EC

For some sectors, the general Data Protection Directive may not provide sufficient legal protection, given specific vulnerabilities or particularities. For the sector of electronic communications, the EU has considered it necessary to supplement the general Data Protection Directive with a sector-specific data-protection directive, which was part of a larger set of directives regulating the electronic-communications sector (formerly known as the telecommunications sector). This is Directive 2002/58/EC.[30]

4.3.1 Relation to 95/46/EC

Directive 95/46/EC must be viewed as the 'lex generalis' which is applicable to the processing of personal data unless a 'lex specialis' determines otherwise. Directive 2002/58/EC (hereinafter: E-Privacy Directive) can be considered to be such a 'lex specialis'. This Directive offers a sector-specific regime with regard to privacy and electronic communications. This means that only those situations regarding processing of personal data that are not covered by the E-Privacy Directive fall within the scope of Directive 95/46/EC. However, from article 1 paragraph 2 it follows that the provisions of Directive 2002/58/EC particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons, such as businesses and foundations. According to article 1, paragraph 1, Directive 2002/58/EC:

> "harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community".

Moreover, article 2 explicitly states that the definitions of Directive 95/46/EC, as well as those of Directive 2002/21/EC concerning a common regulatory framework for electronic communications networks and services, shall apply regarding Directive 2002/58/EC. However, in addition to these directives, a definition is given of some specific personal data that are of great importance to LBS: 'location data' and 'traffic data'.

4.3.2 Location data, traffic data, and their relation to personal data

In article 2 of the E-Privacy Directive, definitions are given of traffic data and location data:

> "(b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
>
> (c) 'location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service."

Since traffic data include data on the geographical position of the terminal equipment at the beginning and at the end of a communication, e.g., a mobile phone call, some traffic data are location data.

[30] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) *OJ* L 201/37, 31.7.2002.

Conversely, many location data in the electronic-communications sector are traffic data, namely if they are processed for the purpose of the conveyance of a communication. This does not necessarily apply to all location data: it is not certain that location data of a mobile phone in stand-by mode can be considered to be processed 'for the purpose of the conveyance of a communication'. On the one hand, the network processes the location of the mobile phone in stand-by mode so that it knows where it should transmit a potential communication to, and in that sense it could be considered to process the location for the purpose of conveying communications. On the other hand, it does not process the location data for the purpose of conveying *a specific* communication; it may well happen that there will be no communication at all in a stand-by session. The categorisation of 'stand-by' location data is therefore a fairly open issue that Member States have to decide upon when implementing the directive.

The Article 29 Working Party has paid attention to the relation between location data and personal data, claiming: *"Since location data always relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in Directive 95/46/EC"*.[31] We consider this too sweeping a statement, since 'location data' (i.e., indicating the location of a user's terminal equipment) can relate to objects that are not linkable to individual natural persons (see below).

To illustrate the complex relation between personal data, location data and traffic data the following figure can provide some clarification.

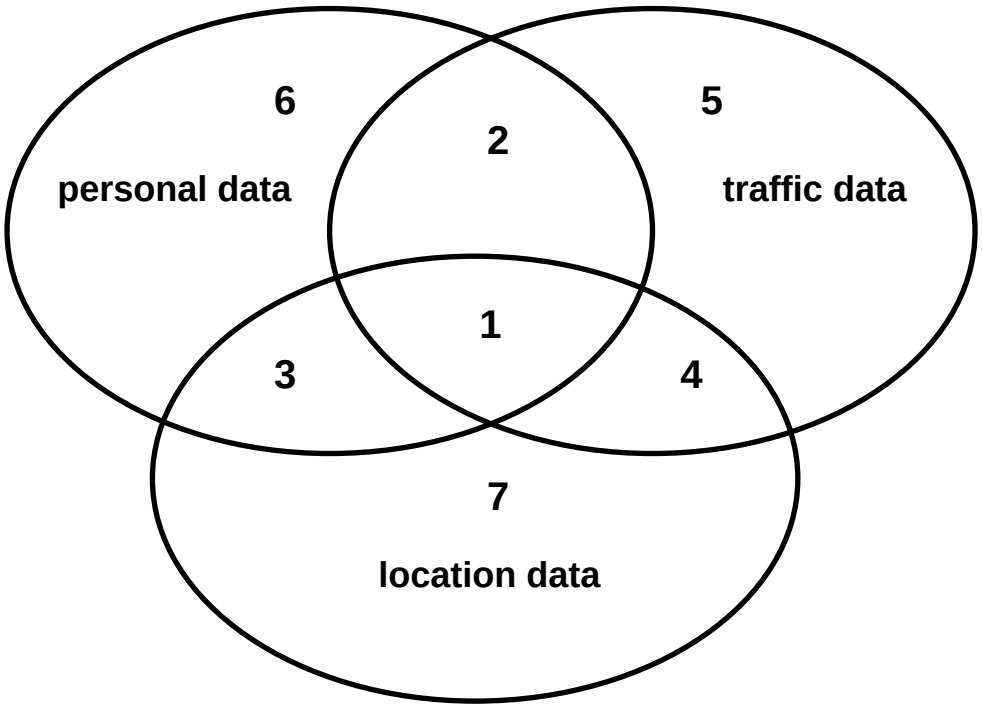

Figure 4. Venn diagram showing the relation between personal, traffic, and location data

1. Location data that are also personal and traffic data, e.g., the cell-ID of a mobile phone used for sending an SMS by an individual subscriber.

[31] Working Party 29, *Opinion on the use of location data with a view to providing value added services*, WP 115, November 2005, p. 3.

2. Traffic data that are also personal data but not location data, e.g., the date and time of a call made by an individual with a GSM subscription.
3. Personal and location data, but not traffic data, e.g., the address of a fixed telephone of an individual.
4. Traffic and location data, but not personal data, e.g., the location of a public phone booth where someone made a call.
5. Traffic data, but not personal or location data, e.g., the date and time when an Internet user accessed a business website using an anonymising service.
6. Personal data, but not location or traffic data, e.g., the account number of an individual.
7. Location data, but not personal or traffic data, e.g., the GPS location of a company car when the company has not registered the actual driver; in the context of electronic communications, possibly the location of a stand-by mobile company phone used by several employers is an example of this category.

This is a schematic representation in which the size of the areas in the figure does not suggest anything about reality. Category 6, of course, is very large, whereas categories 4 and 7, if we follow the opinion of the Article 29 Working Party, are empty, since they consider all location data to be personal data. In our opinion, location data that are not personal data do exist, but this category is probably quite small.

Before we move on to indicating which directives apply to which areas of our Venn diagram, we analyse in more detail the definitions of the various categories of data.

4.3.3 Electronic communications and location technologies

Whether or not certain data are to be qualified as traffic data mainly depends on the question: what is to be understood by *communication* and *electronic communications network?* Besides the definition of electronic communications network, for the qualification of location data the definition of *publicly available electronic communications service* is also of importance. These definitions determine whether the data generated by the various technologies identified in chapter 3 can be considered traffic and/or location data.

The definitions of electronic-communications networks and services cannot be found in Directive 2002/58/EC, but are explained in article 2 of Directive 2002/21/EC.[32]

> "(a) electronic communications networks means transmission systems which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, networks used for radio and television broadcasting and cable television networks;
>
> (c) electronic communications service means a service, normally provided for remuneration, which consists in the conveyance of signals on electronic communications networks. Services providing, or exercising editorial control over, content transmitted using electronic communications networks and services are excluded;
>
> (d) public communications network means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services".

A definition of communication is given in article 2 (d) of Directive 2002/58/EC:

[32] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive"). *OJ* L 108/33, 24.4.2002.

> "(d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information".

The relevant question for study is whether the technologies described in chapter 3 fit these definitions. As described in the technical chapter, a division can be made between satellite-based positioning systems; sensor-based systems; other wireless technologies; cell-based mobile communication networks, and chip-card-based payment systems.

The table below provides insight into which technologies fall within the scope of Directive 2002/58/EC.

	Satellite-based positioning systems like GPS	**Sensor-based systems**	**RFID**	**WiFi**	**Bluetooth**	**Cell-based mobile networks like GSM and UMTS**	**Chip-card-based payment systems like credit cards**
Electronic comm. network	Yes	No (2)	Yes	Yes	Yes	Yes	No (2)
Electronic comm. service	Yes	No (2)	Yes? (4)	Yes? (4)	Yes? (4)	Yes	No (2)
Public	Yes (1)	? (3)	? (3)	? (3)	? (3)	Yes (1)	Yes
2002/58/EC applicable?	Yes	No (2)	If public Yes	If public Yes	If public Yes	Yes	No (2)

Table 3: Relation between LBS technologies and Directive 2002/58/EC

(1) With regard to Satellite-based positioning systems and Cell-based mobile communication networks in general, it can be stated that these are public, in a sense that they are available to the public at large. However, from a technical perspective it is possible, and in view of specific electronic communication services probably already effective, to restrict the access to these networks and services to such a confined group of users that 'public availability' no longer exists, leading to the consequence that Directive 2002/58/EC might no longer be applicable. The lack of clarification regarding the scope of the term 'public' is discussed under (3).

(2) Whether sensor-based systems and chip-card-based payment systems fall within the scope of the definitions of communication networks and services is highly questionable. In our view, if the rationale behind Directives 2002/21/EC and 2002/58/EC is considered, as well as the recitals and provisions of these Directives, the conclusion should be that they are not aimed at such systems. The Directives seem to be aimed at intentional communications in which the content of the communication plays an important role. However, an analysis of the definitions of electronic communications networks and services as well as the definition of communication shows that they are very broad in scope, leaving room for application to sensor-based systems and chip-card-based systems. Even though the definition of communication applies to these systems, since signals are being transmitted by one of the technical means mentioned in the definition of electronic communications service, the person

to whom the data relates has no influence regarding the communication. Therefore, we are of the opinion that it is fair to assume that it was not intended to bring these kinds of systems within the scope of the European legal framework regarding electronic communications. The difficulties with regard to the scope of the definitions of 'electronic communications services', and 'to provide an electronic communications network' are acknowledged by the Article 29 Working Party:

> "These definitions are still not very clear and both terms should be explained in more details in order to allow for a clear and unambiguous interpretation by data controllers and users alike. The unclear definitions give rise to several questions such as for instance 'can a cyber café be considered as a provider of an electronic communications network'? Although such questions should be easy to answer, this is not always the case."[33]

Hopefully, if clarification of these definitions is taken up, the problems regarding applicability to sensor-based systems and chip-card based payment systems will be clarified as well.

(3) In European legislation, there is no definition of what 'public' in the context of the European regulatory framework for electronic communications exactly means. The Article 29 Working Party has not given a clarification regarding the scope of the term 'public'. However, in a recent opinion the Working Party emphasised:

> "The fact that provisions of the ePrivacy Directive only apply to provision of publicly available electronic communications services in public communication networks is regrettable because private networks are gaining an increasing importance in everyday life, with risks increasing accordingly, in particular because such networks are becoming more specific (e.g. monitoring employee behaviour by means of traffic data). Another development that calls for reconsideration of the scope of the Directive is the tendency of services to increasingly become a mixture of private and public ones." [34]

In this respect it is questionable whether the requirement of 'public' networks and services will be upheld in the future. Evidently, it would broaden the scope of the European legal framework regarding electronic communications to a large extent if this requirement is lifted.

For the time being, some relevant criteria regarding the question whether or not a network or service should be considered 'public' can be: the rationale behind legislation; whether or not the network or service is explicitly labelled as 'public' by the legislator; the scope of the service provision: is it the provider's intention to offer the service to anyone who requests this service?; standardisation, which suggest an intention of uniform and public accessibility; whether the network or service is oriented at a limited geographical area[35]; and whether the network or service is specifically aimed or designed for a specific group of people.[36]

(4) RFID, WiFi and Bluetooth are fairly general technologies that transmit data in a wireless way. As such, they fall within the very wide definition of electronic communications network, since they concern a transmission system to convey signals by electromagnetic means. Often,

---

[33] Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive. Adopted on 26th September 2006, 1611/06/EN WP 126, p. 3.
[34] Idem.
[35] In this respect, WiFi networks can be illustrative. If 'public' means accessible for anyone who wants to gain access, a WiFi network can be viewed as 'public', as everyone who is near such a network can in principle gain access to this network. If 'public' means accessible to everyone in the country, then local networks such as WiFi networks can not be viewed as 'public'. It is not yet clear whether or not a geographic limitation prohibits qualifying a network or service as 'public' in the Netherlands. Koops B.J. et al 2005. Aftapbaarheid van Telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet, november 2005, p. 34.
[36] These criteria are derived from Van der Hof S. et al 2006. Openbaarheid in het Internettijdperk. De invloed van ICT op juridische concepten van openbaarheid, Den Haag: Sdu Uitgevers 2006, p. 152 -153.

applications using RFID, WiFi and Bluetooth will also conform to the definition of electronic communications service, if the application can be considered a service.[37] In most cases, these technologies are embedded in some sort of system that can be considered a service, if we go by the general meaning of this term.

4.3.4 Processing of traffic data

The main provisions in Directive 2002/58/EC regarding the processing of traffic data and location data concern articles 5, 6 and 9.

Article 5 concerns the confidentiality of communications and the related traffic data. In this article it is stated that in essence the communications and related traffic data by means of a public communications network and publicly available electronic communications services are confidential. Member States are required to implement this provision into national legislation. In particular, eavesdropping, wiretapping, storage or other kinds of interception or surveillance of communications, by persons other than users, is prohibited without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).

Article 6 of the E-Privacy Directive lays down the ground rule for the processing of traffic data 'relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service'. These data must be erased or made anonymous as soon as they are no longer needed for the purpose of the transmission of a communication.[38] Under certain conditions an exception to this rule is made for traffic data that are necessary for the purposes of subscriber billing and interconnection payments as well as for traffic data for the purpose of marketing electronic communications services or for the provision of value-added services. However, certain conditions apply to these exceptions: the duration of the processing must be restricted to what is necessary to perform the task or service; the subscriber or user must be informed of the types of traffic data which are processed and of the duration of such processing; and, the processing is only allowed by persons acting under the authority of providers of the public communications networks and publicly available electronic communications services. Besides these specific exceptions, the general exception clause of article 15 also needs to be taken into account. This article will be discussed in section 4.3.6.

As described in section 4.3.2, traffic data can, in several instances, be considered to be personal data. If so, the regime set out here supplements the rules laid down by Directive 95/46/EC, meaning that the rights and obligations laid down in this directive also need to be taken into account when processing the 'personal traffic data'.

So, in addition to the specific rules laid down in Directive 2002/58/EC, the general provisions regarding the processing of personal data, such as the obligation to inform as laid down in articles 10 and 11 and the rights to access and to object as described in the articles 12 and 14, are applicable to personal traffic data.

[37] The term service as such is not defined within this directive, nor in the other directives that constitute the common regulatory framework for electronic communications networks and services.
[38] Note the this provision is to a large extent rendered obsolete by the Data Retention Directive, see section 4.3.7.

4.3.5 Processing of (non-traffic) location data

Article 9 of Directive 2002/58/EC concerns the processing of location data other than traffic data. As described before, location data usually can be qualified as personal data. So, for these data the obligations and rights laid down in directive 95/46/EC apply besides the specific provision in the E-Privacy Directive. For location data that are not personal data, e.g., relating to telecommunications subscriptions by legal persons, only Directive 2002/58/EC applies.

Article 9 states that location data other than traffic data 'relating to users or subscribers of public communications networks or publicly available electronic communications services' may only be processed if the data are made anonymous, or with the consent of the users or subscribers of the service to the extent and for the duration necessary for the provision of a value added service. Paragraph 2 of this article states that, if there is consent of the users, there has to remain the ability for the user to refuse the processing temporarily. This provision makes clear that, for the processing of location data, it is required that there is a value added service that cannot be provided without this processing. In addition, the processing has to be limited to the duration necessary to provide this service. So, with regard to location data other than traffic data, unnecessary processing is prohibited, unless the derogation of article 15 applies to the situation.

4.3.6 Article 15: exceptions for national security and law enforcement

As already mentioned in the articles 5, 6, and 9, article 15 provides for some exceptions to the general rules:

> "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph."

This article mainly relates to the use of traffic and location data by public authorities for purposes of safeguarding national security and law enforcement. It allows Member States to pass legislation to allow access of public authorities to such data and to mandate data retention, without consent of data subjects. For data retention, there is a specific directive, which we describe in the next section.

Whereas Directive 2002/58/EC prescribes consent of the data subject or a legally authorised situation as mentioned above, Directive 95/46/EC also offers a weighing of the relevant interests to justify processing of personal data (art. 7(f)). The absence of this ground in Directive 2002/58/EC means that this option does not apply to location data or traffic data generated solely because of electronic communications. Therefore, in private relationships, only consent remains as a legal ground for the processing of these data. According to the definition in article 2(f), 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC. The data subject himself therefore has to give the prior informed consent. In a workplace environment, there can be an exception to this, see section 4.7.

4.3.7 Data Retention: Directive 2006/24/EC

Directive 2006/24/EC (hereinafter: Data Retention Directive) regulates the mandatory storage of traffic data (cf. art. 15 of the E-Privacy Directive). These data need to be stored by service and network providers in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The Directive only concerns traffic data; the content of the messages is excluded from the obligation of data retention. Traditionally, such a regulation in the field of law enforcement falls outside of the competence of Directives (an instrument in the First Pillar of the EU which deals with the internal market); however, data retention closely relates to the functioning of the common market, and the diverging rules of Member States on data retention, which 'vary considerably' (consideration 5), form an obstacle to the internal market for electronic communications (consideration 6).

This directive pertains to traffic data, location data, and 'the related data necessary to identify the subscriber or user'. Definitions are the same as those of Directives 95/46/EC, 2002/21/EC and 2002/58/EC (art. 2 para. 1). According to article 4, these data must be retained 'to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.' The data to be retained are specified in article 5 of the Directive, which distinguishes between fixed and mobile telephony on the one hand, and Internet e-mail and Internet telephony on the other. The obligation includes unsuccessful call attempts, i.e., where a telecommunications connection was made but the call was not answered by the recipient, if such data are stored or logged by the provider (art. 5 para. 2).

For this study, particularly the data in art. 5 para. 1 under (f) are relevant:

> "data necessary to identify the location of mobile communication equipment:
>
> (1) the location label (Cell ID) at the start of the communication;
>
> (2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained."

The required duration of storage is at least six months with a maximum of two years (art. 6). The exact period of storage is to be decided upon by each and every Member State in its implementation. The maximum period may even be extended, for a limited period, for Member States 'facing particular circumstances that warrant an extension' (art. 12).

The Data Retention Directive must be transposed in Member States by 15 September 2007, with a possible postponement for Internet data until 15 March 2009 (art. 15).

4.4 Which Directives apply to which kinds of data?

In the previous section, we sketched the complex relationship between personal data, traffic data, and location data as well as the directives and provisions that apply to these data. Generally, the E-Privacy Directive takes precedence over the Data Protection Directive, but the latter, general, directive supplements the protection of traffic and location data when they are not covered by specific provisions in the sectoral directive. Within the E-Privacy Directive, different regimes apply to traffic data and to location data that are not traffic data. The picture is compounded by the fact that the E-Privacy Directive provisions only apply to public communications. Traffic and location data generated by private networks or in private services are not covered by articles 5, 6 and 9; if they relate to individuals, however, the

general Data Protection Directive applies. This leads to a very complex picture of applicability of legal provisions to the various kinds of data. We tentatively represent this in Figure 5, which may serve as a working tool for further analysis.

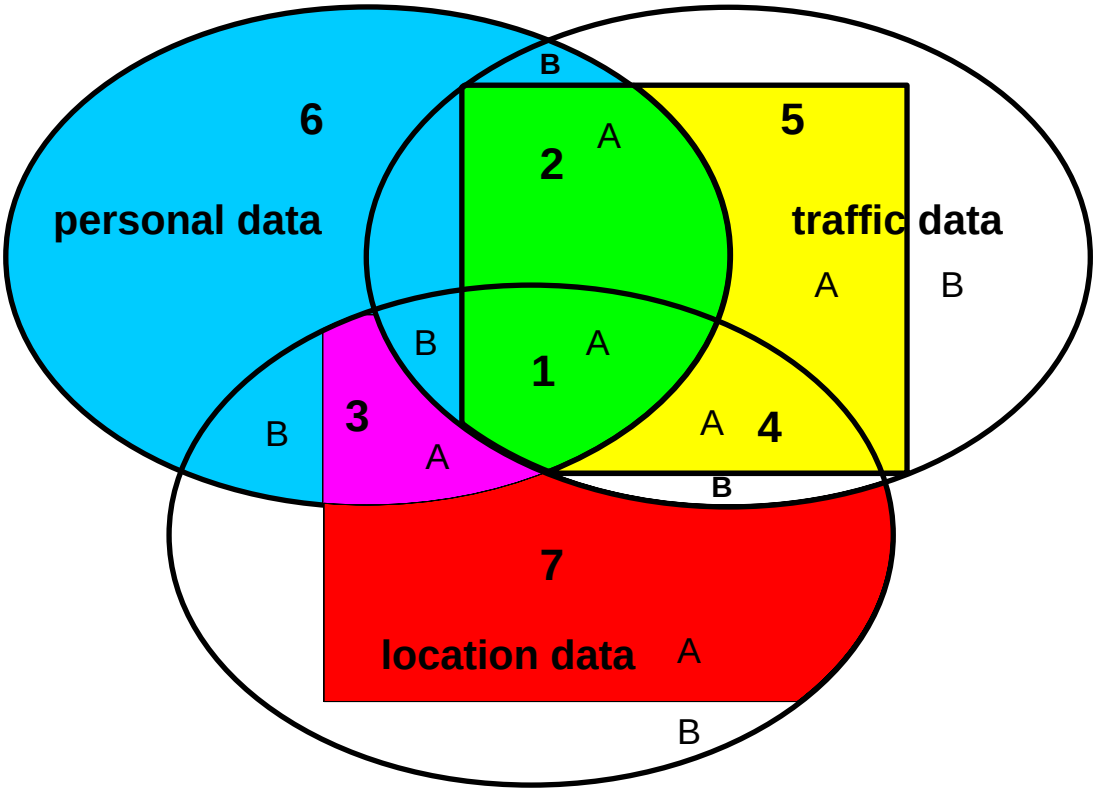

Figure 5. Diagram showing the applicability of Directives to data

In Figure 5, yellow indicates applicability of articles 5 and 6 of the E-Privacy Directive, red indicates that article 9 of this directive applies[39]. Blue indicates the scope of the general Data Protection Directive. The purple (red + blue) and the green (yellow + blue) part show that for some data, the specific provisions of the E-Privacy Directive as well as the general Data Protection Directive apply. As can be seen, and is furthermore explained below, this is only the case in public networks or services (indicated with an 'A').

'A' denotes that the data are generated in public networks or services, 'B' that they are generated in private networks or otherwise fall outside the scope of the E-Privacy Directive, for instance because they do not relate to electronic communications at all.

1. The category of traffic data that are also location and personal data, is divided in two subcategories.
    a. For data generated in public networks or services, articles 5 and 6 of the E-Privacy Directive apply, indicating requirements such as confidentiality, the legal grounds for processing, storing, and erasure. Other requirements from the Data Protection Directive also apply, when they relate to personal data and are not specifically covered by the E-Privacy Directive, such as several aspects of data quality and data security (art. 6 and 17 Data Protection Directive).

[39] Note that we do not follow the Opinion of the Article 29 Working Group here, which claims that all location data are personal data. That is not the case; see section 4.3.2.

   b. For other data, i.e., those generated in private networks or services, only the general Data Protection Directive applies.
2. The category of personal and traffic, non-location data is divided in two subcategories.
   a. The same as category 1a.
   b. The same as category 1b.
3. The category of location and personal, non-traffic, data is divided in two subcategories.
   a. To data generated in public networks or services, art. 9 of the E-Privacy Directive applies, as well as other requirements from the general Data Protection Directive not covered by the E-Privacy Directive.
   b. To other data, only the general Data Protection Directive applies.
4. The category of traffic and location but non-personal data, e.g., relating to business subscriptions, is divided in two subcategories.
   a. To data generated in public networks or services, only articles 5 and 6 of the E-Privacy Directive apply.
   b. Other data are not covered by any legal data-protection instrument.
5. The category of traffic, non-location, non-personal data is divided in two subcategories.
   a. The same as category 4a.
   b. The same as category 4b.
6. To personal data which are not traffic or location data, only the Data Protection Privacy Directive applies.
7. The category of location, non-traffic, and non-personal data is divided in two subcategories.
   a. To data generated in public networks or services, only article 9 of the E-Privacy Directive applies.
   b. Other data are not covered by any legal data-protection instrument.

4.4.1 Checklist

From the foregoing it can be concluded that providers of LBS have to ask a lot of questions before they can determine what regime is applicable to the data they are processing in order to provide the LBS. To help providers asking the right questions, we provide a checklist of the relevant questions that need to be answered in order to establish the applicable legal regime.

1. Are the data to be processed 'personal data'? (see art. 2(a) of Directive 95/46/EC)
2. Are the data to be processed 'traffic data'? (see art. 2(b) of Directive 2002/58/EC)
3. Are the data to be processed 'location data'? (see art. 2(c) of Directive 2002/58/EC)
4. Do the data relate to users or subscribers of public communications networks or publicly available electronic communications services? (see art. 6 and 9 of Directive 2002/58/EC and art. 2 (a), (c) and (d) of Directive 2002/21/EC)
5. Is one of the exceptions applicable? (see article 13 of Directive 95/46/EC and article 15 of Directive 2002/58/EC).

4.5 The legal framework in practice

4.5.1 Introduction

After the clarification of the European legal framework regarding the processing of personal data, traffic data and location data, this section will elaborate upon some relevant distinctions and problems that exist with regard to applying these Directives in practice. As described before, the processing of location data occurs in the context of providing Location Based

Services. In the described directives, no definition is given of a Location Based Service. However, in article 2(g) of the E-Privacy Directive, a value-added service is defined as:

> "any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof."

Location Based Services are a subset of Value-Added Services. They could be defined as:

> "any service which requires the processing of locational traffic data or location data that are not traffic data etc."

As a result, the legal framework regarding value-added services is also applicable to Location Based Services.

As already mentioned, LBS can be public as well as private in nature, and can be used by public and private parties as well. The provision of these services can be either direct or indirect by nature, and also the access to the data generated when providing LBS can be accessed directly as well as indirectly. Besides these distinctions, this section will also provide insight into the problems that can arise in hierarchical relationships, as one of the main grounds for the processing of location data is consent. In this respect, it is also of interest to highlight the problem of who should consent to the processing of certain data: the user, the subscriber, or both?

4.5.2 Public and private relationships

From the description of the European legal framework it becomes clear that there is a big difference in the exceptions regarding the processing of location data for private parties and public parties. Because of these differences, a distinction between the two is made throughout this study. At the end of this chapter, two specific relationships will be discussed more elaborately as some specific legislation and problems relate to them. In section 4.6, the access to traffic and location data by law enforcement will be described, while section 4.7 will give an insight into the processing of traffic and location data by employers.

In private relationships, commercial interests, such as the provision of value-added services, are one of the main reasons for generating location data. However, also the safety of children and elderly people can be mentioned as private interests to process location data. The localisation of elderly people and children is a sound example of relationships in which the subscriber to the service is not the same person as the one who is being located. The same holds true for employment relationships, in which the employer will often be the subscriber to a service, while his employees will be the ones to be located. This difference is of importance in relation to the question who should consent to the processing of certain data, the subscriber or the user?

4.5.3 Subscriber, user, and the consent to be given

Contrary to the processing of personal data on the basis of Directive 95/46/EC in which article 7 provides several legal grounds, such as a weighing of the interests (article 7 (f)), section 4.3 made clear that the processing of traffic data and location data heavily depends upon consent. Article 2 (f) of the E-Privacy Directive states: *"consent by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC"*. Article 2 (h) of this directive defines 'the data subject's consent' as meaning: *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."*

From the definition in the E-Privacy Directive it becomes clear that consent must be given by either the subscriber, the user or both. In article 2(a) of Directive 2002/58/EC a definition is given of a 'user': *"any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service"*. A definition of a subscriber cannot be found in this Directive. However, article 2(k) of Directive 2002/21/EC defines 'subscriber' as: *"any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services."*

First, the relevance of the distinction between user and subscriber relates to the fact that subscribers can be legal persons as well as natural persons. This means that the scope of Directive 2002/58/EC is broader then the scope of Directive 95/46/EC, which is aimed at natural persons. Second, this distinction is relevant as the data being processed in order to provide value-added services do not necessarily have to relate to the subscriber to the service, but they can also relate to a user. For example, within a family a father can have a subscription to a service that locates the mobile phone of his children. In this situation the father is the subscriber, while the children are being the users. Also within an employment relationship, the employer – being a legal or a natural person – can be the subscriber to a service locating company vehicles in order to avoid traffic jams. However, not the employer, but the employees are the users of this service when driving the company vehicle. A third relevant issue regarding the distinction between subscriber and user relates to article 6(2) of the E-Privacy Directive which concerns an exception to process traffic data necessary for the purposes of subscriber billing and interconnection payments. Processing of these data is allowed, but only with regard to subscribers of a service, not regarding its users.

Recital 31 of the E-Privacy Directive gives an insight into the question from whom consent should be obtained:

> "Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it."

On the basis of the definition of consent as laid down in the Data Protection Directive, as a general rule, the data subject has to give his or her consent. This implies that in the case of a subscriber using a location based service in order to track and trace users of certain equipment such as a phone or a GPS-equipped vehicle, consent needs to be given by both the subscriber as well as the user. The Working Party takes the view that, when a service is offered to private individuals, consent must be obtained from the person to whom the data refer, i.e., the user of the terminal equipment.[40] With regard to providers of value-added services, the Article 29 Working Party has explicitly stated that they must take appropriate measures to ensure that the person to whom the location data relate is the same as the person who has given consent.[41]

From the definition of consent, as well as from articles 6 and 9 of the E-Privacy Directive, it becomes clear that consent can only be given on the basis of complete and accurate information. The Article 29 Working Party takes the view that information should be provided by the party collecting the location data for processing, i.e., by the provider of the

[40] Working Party 29 2005, note 31, p. 7.
[41] Idem, p. 6.

value-added service or, where the provider is not in direct contact with the data subject, by the electronic communications operator.[42]

Information does not only need to be given at the time that consent is obtained, but subscribers should be kept informed on a regular basis whenever a service requires on-going processing of location data. Information should not only be given about the fact that terminal equipment is being located, but also a reminder should be given of the possibility to withdraw consent at any given time.[43] This follows from the articles 6(3) and 9(1) of Directive 2002/58/EC that explicitly require that the users (or subscribers) have to be *"given the possibility to withdraw their consent for the processing of traffic data at any time."* Article 9(2) states that

> "for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication."

This requirement might raise problems in relation to new communication technologies. At this moment, there are already cell phones available that can be traced on their transmission signals, even when they are turned off. In this situation, it is questionable if a user can be excluded from localisation.

In case a subscriber is using the service to track and trace other users, it is fair to assume that the duty to inform the user will be on the subscriber. To a certain extent, this can be found in Recital 17 of Directive 2002/58/EC. This recital mentions that consent means the same as consent in Directive 95/46/EC. Furthermore, it says: "Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes". The wishes of the user are the main objective, implying that at least there has to be knowledge by the user so he is able to express his wishes to the subscriber.

The way in which consent should be given, is also a question open to discussion. With regard to the processing of location data the Article 29 Working Party has stated that the definition of consent as described in Directive 95/46/EC explicitly excludes consent being given as part of the acceptance of general terms and conditions for the electronic communications service offered. However, depending on the type of service offered, consent may relate to a specific operation or may constitute agreement to being located on an on-going basis.[44]

The problems that exist regarding consent in hierarchical relationships will be further elaborated upon in section 4.7 concerning employment relationships.

4.5.4 Direct and indirect provision of services

The first services offered on the basis of location data involved requests from subscribers or users regarding the availability of certain facilities near to them, for example the nearest hospital. Nowadays, value-added services are also provided the other way around, on the request of a third party. For example a restaurant that wants to send commercial text messages to nearby mobile phones, hoping to attract customers. In this example, the restaurant will probably make use of the services provided by an electronic communications operator. This means that at the request of a third party, location data needs to be processed by another third

[42] Idem, p. 5.
[43] Idem, p. 7.
[44] Idem, p. 5.

party, concerning certain nearby individuals. This difference is also described by the Article 29 Working Party:

> "A value-added service based on location data can be provided either directly by the electronic communications operator (the individual concerned contacts the operator, who then provides the service on the basis of the location data obtained from his system) or via a third party (the individual concerned contacts a third party, who then provides the service on the basis of the location data obtained from the operator)".[45]

In other words, direct provision of services means that the data subject connects to the operator who provides the value-added service based on location data from his own system, whereas indirect provision means that the user connects to a third party who provides the service based on location data obtained from the operator. In this case, the provider of the service needs to obtain consent from the subscriber or the user. The service provider requests to receive the location data from the other operator. Of course, this request is not necessary in the case the terminal equipment produces the location data.

4.5.5 Direct access to location data

If the provider of a value added service has direct access to the location data of users, further transfer of data is not necessary to provide the service. This is the case in two-party structures, using, for example, RFID. The provider, who owns the RFID Reader, can provide his services on the basis of location data gathered by his own system. This means that a user has to give his prior informed consent to the provider with regard to the use of his location data.

As described in the previous section, a request for disclosure of location data can also be done by a service provider to a mobile operator in case of a three-party structure. In these structures, such as Cell-ID, a third party provides a network that generates the location data. The user of a service gives his prior informed consent to the provider of the service. This provider has to receive location data from the network provider. In these situations, consent to use location data in order to provide a value-added service also needs to involve consent to transfer the location data from one provider to the other. The communications operator is only allowed to provide the location data if the service provider has the consent of the subscriber and/or the user to process his traffic and location data.

In relation to this, the definition of 'processing' can be important. In European Member States, 'processing' is interpreted in different ways. Some Member States include mere transfer of data in processing, while others do not. This means that for the transfer of location data from a mobile operator to a provider of a value-added service, not all Member States require consent of the data subject.

In case a provider of value-added services needs to request location data from an electronic communications operator, the Article 29 Working Party stresses the need for the operator to verify and authenticate such requests for access to location data.[46] It is also suggested that the data are provided by the operator in such a way that the service provider cannot identify the customer (e.g., by using an alias).

[45] Idem, p. 6.
[46] Idem.

4.6 European legal framework for accessing location data by law enforcement

In the EU, there is no general legal framework for law-enforcement powers, since this is an issue still left to Member States to regulate. Only for some specific measures is there considered to be a need for harmonisation, for example, for data retention (see above, section 4.3.7), and for criminalisation of attacks on computer systems.[47] The Data Retention Directive contains one relevant provision in this respect, article 4: *"Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law."* This does not provide guidance for national law on the conditions under which law enforcement agencies can access location data, however.

For such guidance, we need to look at the Council of Europe.[48] The general legal framework here is the European Convention on Human Rights and Fundamental Freedoms (ECHR), in particular article 8. This provision protects the right to private life and, among other things, correspondence. Law-enforcement powers to access personal data have to fulfil the requirements of article 8, paragraph 2: they must be established by law and be foreseeable for citizens, in the interest of, among other things, national security or crime prevention, and they must be 'necessary in a democratic society'. This implies a proportionality test, but leaves a fairly wide margin of appreciation for European states to establish law-enforcement powers.

More specific provisions are found in the Council of Europe Convention on Cybercrime (CCC).[49] This convention entered into force on 1 July 2004 for those states who ratified it. As of February 2007, the convention has 19 party states.[50] The convention needs to be implemented by the party states in their national laws.

The general provision to access location data is the article relating to real-time collection of traffic data. Party states should establish a power for law enforcement to collect or record, with the help of service providers, *'traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system'*. This power should be usable at least for cybercrimes, but preferably for all crimes where electronic evidence is relevant (art. 14 CCC). It should also be used in cases where mutual legal assistance is required, i.e., when a party state requests another party state collect real-time traffic data (art. 33 CCC).

For location data that are not traffic data (categories 3 and 7 in Figure 1), the powers of a production order (art. 19 CCC) and search and seizure of stored computer data (art. 19) may be used. The Explanatory Memorandum explains that the production order may also cover the fixed location data of end equipment.[51] A crucial difference with the traffic-data regime is that

---

[47] Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ* L69/67, 16.3.2005.
[48] For those unfamiliar with this European organisation, see: <http://www.coe.int/T/e/Com/about_coe/>.
[49] Convention on Cybercrime, Budapest, 23 November 2001 (ETS 185), available at: <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.
[50] See: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.
[51] "[T]he site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement. This latter information may only be relevant in practical terms where the equipment is not portable, but knowledge as to the portability or purported location of the equipment (…) can be instrumental to an investigation." Explanatory Memorandum to the Convention on Cybercrime, available at: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>, § 180.

traffic data should be provided by service providers *in real-time*, contrary to other kinds of data.

Since traffic data are volatile, the convention also contains powers to command the preservation of specific data, including traffic data, for a maximum period of 90 days (art. 16 CCC). This is not a sweeping *ex-ante* data-retention measure, since it regards only data specifically designated *ex-post* in concrete cases. It is not relevant for EU member states, where data retention is mandatory anyway, except perhaps in very rare cases where law enforcement needs to obtain traffic data just when the mandatory data-retention period is about to expire. It may also be relevant, however, for location data that are not traffic data, e.g., data generated by certain GPS applications.

4.7 European legal framework for processing location data by employers

4.7.1 Introduction

According to case law of the European Court of Human Rights (ECtHR), also in the workplace, some reasonable expectation of privacy exists. In the Halford case, the ECtHR considered that the border of this privacy expectation depends on the circumstances the employee might and could have expected on beforehand.[52] In accordance with the applicability of Article 8 of the European Convention on Human Rights and Fundamental Freedoms within employment relationships, also the European Directives regarding the processing of personal data are applicable within these relationships.

The Article 29 Working Party has already on several occasions drawn attention to the specific problems that arise with regard to the processing of personal data within employment relationships. In 2001, opinion 8/2001 on the processing of personal data in the employment context was adopted,[53] followed by a working document on the surveillance of electronic communications in the workplace.[54] In the opinion on the use of location data with a view to providing value-added services, a specific section is reserved for the location of employees.[55]

In the latter opinion, it is stated that the processing of location data raises two issues: "*the dividing line between work and private life and the degree of monitoring and permanent surveillance to which it is acceptable to subject an employee.*"[56]

With regard to the lawfulness of the processing of location data, attention is given to consent of the employee. As consent constitutes the main problem regarding processing of personal data in employment relationships, the next section will provide some further insight into this issue. Other points of interests raised by the Article 29 Working Party relate to the requirement that processing of location data on employees must correspond to a specific need on the part of the company which is connected to its activity; the fact that the purpose of the processing must not be achievable by less intrusive means; equipment should offer the possibility to switch the location function of, as employers should not collect location data

[52] ECtHR, 25 June 1997, NJ 1998, 506 (Halford/UK).
[53] Opinion 8/2001 on the processing of personal data in the employment context Adopted on 13 September 2001, 5062/01/EN/Final WP 48.
[54] Working document on the surveillance of electronic communications in the workplace 5401/01/EN/Final WP 55.
[55] Working Party 29 2005, note 31, p. 9.
[56] Working Party 29 2005, note 31, p. 10.

relating to an employee outside his working hours; a reasonable retention period should not supersede two months; employers should take adequate measures to restrict and secure access to location data; and employees should be properly informed regarding (the possibility) to be monitored.

4.7.2 Consent

As already mentioned, the processing of location data in hierarchical relationships can be problematic as consent is the sole legal ground for the processing of these data, at least as far as no exception is applicable. In law enforcement, several of these exceptions apply, but in private relationships only billing purposes are mentioned as an exception to the general rule that consent is required.

In this respect, the statement of the Article 29 Working Party in its opinion regarding the processing of location data is somewhat strange: *"Such processing should not rely exclusively on the employee's consent, which must be 'freely given'."* The next sentence in the opinion does not really clarify the issue:

> "As already pointed out by the WP in its working document on data protection in the employment context, the issue of consent should be addressed in a broader perspective; in particular, the involvement of all the relevant stakeholders (as envisaged in the legislation of several Member States) via collective agreements might be an appropriate way to regulate the gathering of consent statements in such circumstances."

The fact remains that consent is the only ground for the processing of location data. Therefore it is fair to assume that the statements of the Working Party probably address the way in which consent should be given. For an employment context, it is questionable whether consent for the processing of personal data can be integrated in the employer's labour contract. By incorporating the processing into the contract, the employee might not specifically consent to the processing. The reason to sign the contract is because the employee wants to be hired, and thus he signs the contract containing clauses regarding the processing of his personal data. If he does not sign the contract he might not be hired, so his consent to the processing might not be freely given. From the statement of the Article 29 Working Party mentioned above, as well as from opinion 8/2001, it can be concluded that the Party rejects the processing of personal data within the employment relationship when this processing is solely based on consent incorporated into the individual labour contract. For larger companies the Article 29 Working Party expressed that use of a works council can be a helpful tool to arrange agreements on a central level.[57]

Another peculiarity in relation to consent relates to the difference in 'normal' consent and unambiguous consent. As mentioned before, art. 2(h) of the Data Protection Directive defines consent as: *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."*

If consent is used as a ground for the processing of personal data as described in article 7(a) of Directive 95/46/EC, consent must be given 'unambiguously'. However, in case of the processing of location data, article 9 of the E-Privacy Directive is applicable, requiring consent without the requirement of it being given unambiguously.

[57] Opinion 8/2001 on the processing of personal data in the employment context, WP 48, p. 23.

4.7.3 Direct and indirect access to location data

Also in the context of an employment relationship, a distinction needs to be made between location data collected and stored by a third party, such as a telephone company or an Internet service provider, and location data collected and stored by an employer himself, for example in an intranet or when using an RFID-tagging system for authorisation purposes. If the employer processes the data himself, the mere question that arises regards the lawfulness of the processing in relation to the (privacy) interests of the employee. However, if the employer uses a third party network or service in order to monitor his employees, he needs to gain access to the location data by requesting them from the third party involved. Here the question that arises is twofold: the lawfulness of the processing of the data as well as the lawfulness of the transfer of these data from the third party to the employer.

4.7.4 Applicability of the European legal framework

Another important issue to take into consideration is the applicability of the European Legal Framework with regard to the processing of location data within private systems deployed by the employer. Because these systems probably will not qualify as 'public' communication or communications service within a 'public' communications network, the E-privacy Directive might not be applicable (Art. 2(d) of Directive 2002/58/EC and Art. 2(a), 2(c) and 2(d) of Directive 2002/21/EC).

4.7.5 User and subscriber

Another important factor within employment relationships concerns the difference between subscriber and user. In general, in the case of a structure in which the employer depends on a third party for the processing of location data, the employer will be the subscriber to the service, but not the data subject or the user of this service. The location data to be processed will relate to the employees, and therefore, they are the data subjects and users of the service, yet they did not subscribe to this service. So, the question as to who needs to consent, and who needs to provide the information in order to satisfy the requirement of informed consent, plays an important role in employment relationships.

In this respect, White[58] makes an interesting distinction between three different instances of using location monitoring systems generating location data.

- Consensual use, in which the employee is a willing participant.
- Non-consensual use, which occurs without the individual's knowledge or permission.
- Flexible use, which covers devices whose use has the unintended consequence of tracking location information.

According to these conditions, non-consensual use, as described above, will be prohibited, and active use will be allowed on the basis of consent, assuming that enough information is provided in order for this consent to be informed, and the hierarchical relationship not being in the way of consent being freely given. Flexible use is more difficult. An example might be that the car of a company has a GPS system to prevent it from being stolen or car-jacked. In this respect, not only the requirements regarding consent must be met, but also the

[58] White J. C., People not places. A policy framework for Analyzing Location Privacy Issues, see: <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf>. White uses the terms 'active' and 'passive' for the first categories; we have rephrased this to prevent confusion with other definitions of 'passive' LBS, see below, note 61.

(im)possibility to turn off the localisation system can play an important role in assessing whether or not the processing of the location data is allowed.[59]

4.8 Conclusion

From our discussion of the various Directives and legal provision pertaining to personal data, traffic data, and location data, it becomes clear that the current legal framework regarding the processing of these data is very complex. The main difficulty with the European legal framework lies with the legal definitions and qualification of different groups of data, the overlap that exists between these groups, and the different legal regimes applicable to the different groups of data. The rules regarding the processing of personal data (Directive 95/46/EC) are complemented with rules regarding location data and traffic data as laid down in Directive 2002/58/EC. This leaves room for all kinds of combinations between personal, location, and traffic data, and the different directives lay down different regimes for all these combinations. In conclusion, it is fair to say that a very complex legal framework for the processing of personal, location and traffic data has been created.

This makes it relevant to look at the implementation of this legal framework in various national legislations. Such a complex framework with not always clear-cut definitions is difficult to implement straightforwardly, and hence, it can be imagined that national legal frameworks differ to a certain extent in their implementations. Also, the interpretation of the various definitions and provisions may differ from country to country, when it comes to applying these to the various technologies and systems used for LBS as outlined in Chapter 3.

In the following chapters, we will study various LBS applications and the national legal framework of four EU countries, in order to compare the implementation and interpretation of the European legal framework in the national legal frameworks of these countries.

[59] Working Party 29 2005, note 31, p. 11.

5 Location Information from a Belgian Perspective

Fanny Coudert & Eleni Kosta (ICRI)

5.1 Introduction

Location data refer to all data which indicate the geographical position of an individual at a defined moment. The processing of location data must, as should all processing of personal data, comply with the provisions of the Data Protection Act.[60] Such data can be obtained through different means, for instance via a smart card used to access a service or when making a phone call via a mobile phone. In this last case, the location of an individual can be obtained through the processing of traffic data, i.e. from the data processed for the transport of communication into an electronic communication network or for the billing thereof, or location data, which means any data processed in an electronic communications network indicating the geographical position of a final user's terminal equipment when he uses a public electronic communications service. The latter may involve information on the latitude, longitude and altitude of the place where the device is situated, the direction of movement, the degree of precision of location data and the identification of the network cell where the terminal device is situated at a given moment.

The spread of Location Based Services provided through public electronic communications networks has raised a series of data protection concerns. Location Based Services represent an emerging market in Belgium since the introduction in 2003 of information services based on the location of the user, with better commercial expectations than the traditional telephony services. The services offered extend from the provision of information upon request relative to services close to the user's location (pharmacies, restaurants, etc.) to the localisation of a mobile phone (employees, children, friends, senior citizens, etc.). The last category of services is known as Passive Location Based Services. They are defined as those services where a mobile phone user, once he has enabled the service, consents to be located by another person, when that other person initiates a location request from another mobile phone or from a PC.[61] Very popular are the so-called Child Location Services that allow the parents to track their children.[62] These services could harm not only the right to privacy of the user, a right constitutionally protected in Belgium, but also his right of movement in an anonymous way, as long as they enable the subscribers to know where the user is at any moment.

Specific provisions have been introduced by the Act of 13 June 2005 relative to electronic communications[63] (hereafter Electronic Communications Act) that complements the general rules provided by the Data Protection Act. However, the rapid evolution of these services has already motivated two law proposals with the purpose of adjusting the provisions of the Electronic Communications Act to these specific situations and in particular for the regulation of employee monitoring.

---

[60] Act of 8 December 1992 on the protection of the privacy in relation with the processing of personal data (*loi relative à la protection des données à caractère personnel*) as modified, *M.B.* (*Belgian Official Gazette*), 18 March 1993, consolidated version available at: <http://www.privacycommission.be>.

[61] Code of Practice for the use of passive location services in the UK, 24 September 2004, available online at: <http://www.themda.org/documents/COP/LBCCodeofPractice050505.pdf>.

[62] See FIDIS D11.2.

[63] Act of 13 June 2005 on electronic communications [*Loi relative aux communications électroniques*], *M.B. [Belgian Official Gazette]* (2nd ed.), 20 June 2005.

Several aspects should be taken into account in order to present the legislation applying to this kind of processing. The general obligations related to personal data processing as they stand in the Data Protection Act will be discussed and complemented, when appropriate, by the specific provisions of the Electronic Communications Act (section 5.2). In several cases, specific legislation should also be taken into account. Regarding the processing of location data by public authorities, an experiment carried out in Flanders on traffic management will be discussed and the provisions applying to processing for law enforcement purposes will be outlined (section 5.3). The specific case of employee monitoring and localisation of a third party's mobile phone will be described (section 5.4), while the research conducted under the auspices of the Institute for BroadBand Technology (IBBT) in Flanders will also be presented (section 5.5).

5.2 Legal framework: general principles

As mentioned above, all personal data processing should comply with the general obligations established by the Data protection Act. The Electronic Communications Act will only apply to location data processing when the data originate from a public electronic communications network. We will then analyse the provisions of data protection legislation regarding the processing of location data and how they should be complemented with the provisions of the Electronic Communications Act. Moreover, we will refer to the law proposal modifying the Electronic Communications Act for ensuring a better protection of private life in Location Based Services or the services based on the location data of mobile phones (hereafter law proposal to amend the Electronic Communications Act)[64], which has already been drafted in order to adapt the Electronic Communications Act to Location Based Services. This law proposal aims at solving the specific issues of Location Based Services, whose purposes consist in locating a third party's terminal equipment, with regard to consent and information of the subscriber and the user.

The processing of location data should comply with requirements regarding the purposes and proportionality of processing, as well as consent, information provision, and rights of the subscribers and users of the services. In this section, we discuss these requirements in some detail.

5.2.1 Purpose specification and proportionality

According to Art. 4-2° of the Data Protection Act, personal data should be collected for specific, explicit and legitimate purposes. This means that the processing of personal data should be based on a legitimate interest of the controller. This will raise specific issues in the field of the processing of location data of workers by the employer (see infra 5.4.1).

Moreover, the data collected should be adequate, relevant and reasonable according to the purposes. This means that the data collected should be proportionate to the purpose of the processing and should not exceed what is strictly necessary. This provision will be especially important with regard to the processing of location data, where the devices which collect the data usually provide more information than necessary for the provision of the service.

[64] Law proposal to amend the Act of 13 June 2005 relative to Electronic Communications, for ensuring a better protection of private life in Location Based Services or the services based on the location data of mobile phones (*en vue d'assurer une meilleure protection de la vie privée pour les services à données de localisation ou les services de géolocalisation par téléphone portable*), Ref doc. Senate 3-1856.

5.2.2 Information provision

The Data Protection Act compels the controller to inform the data subject of his name and address, the purposes of the processing, the recipients or categories of recipients of the data, the existence of a right to object and of the existence of the rights of the data subject (Art. 9).

Article 122 §3 of the Electronic Communications Act introduced a specific obligation of information provision for the processing of location data in the field of electronic communications. It stipulates that Mobile Networks Operators should inform the subscriber or, when appropriate, the final user, before he gives his consent, of the kind of data to be processed, the specific objectives and duration of the processing, the eventual third parties the data that will be transferred, and about the possibility of withdrawing their consent at any moment, definitely or temporarily (Art. 123-1°). According to the preparatory works, the Operators will not have to inform all the users when the subscriber is a legal person, for practical reasons. In these cases, the burden to be put upon the Operator appeared to be disproportionate.[65]

The law proposal to amend the Electronic Communications Act intends to extend this obligation of information to the user of the terminal equipment. It is foreseen that the Operator will be obliged to inform before the subscription to the service both the subscriber and the user, when they are different persons. This modification echoes the opinion of the Belgian Data Protection Authority raising the problem of the consent given by legal persons (in most of the cases, the employer)[66]. The ePrivacy Directive[67] which the Electronic Communications Act transposes into Belgian legislation, is intended to apply to both users and subscribers and therefore the recipients of the obligations set up to the Telecommunication Operator will depend on who the data are related to. According to this principle, Belgian Law could not exclude one of these data subjects from the application of the provisions because of practical reasons.

Moreover, the law proposal compels the Operator to send an information message warning upon the activation of the service for each localisation request. This obligation would ensure that the user is informed of these requests and thus of the processing of location data and enable him to withdraw consent.

5.2.3 Consent

The Data Protection Act lists several grounds on which the data processing can be justified. Even if consent will generally be the most common option, the controller is allowed to process the data without prior consent of the data subject when he can rely, for instance, on a legitimate interest, provided that this interest outweighs the fundamental rights and freedoms of the data subject (Art. 5).

In the field of electronic communications, prior to the processing, the Operator should collect the consent of the subscriber or, when appropriate, of the end user. Article 122§3 of the Electronic Communications Act gives a definition of consent which literally reproduces the definition given by the Data Protection Act: consent is any freely given specific and informed

[65] Ibid.
[66] Opinion n°8/2004 of 14 June 2004, on the draft of Electronic Communication Law.
[67] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.

indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

The law proposal to amend the Electronic Communications Act intends to extend this obligation and to compel the Operator to obtain the consent of both the subscriber and the user. Moreover, this law proposal tries to solve the issue of the services of localisation of minors. The Preamble refers to the issues identified by the Working Party 29[68]. The fear of criminal offences and the emergence of a nomadic way of living could lead parents to use this service for their own reassurance. They introduce the use of mobile phones as part of a family contract: more freedom of communication for the children against the possibility to be localised by the parents. However, this need of the parents should be limited by the right to privacy of the child as mentioned in the Convention on the Rights of the Child[69]. The use of these services could hinder the establishment of a relationship based on mutual trust between the parents and their children and could have a negative impact on the course of the children to gain their autonomy. Moreover, such services could mislead the parents into believing the illusion that they control the activities of their children, when in fact the mobile phone only indicates where this device is and thus supposedly where the child is, but not what he is doing. Finally, the widespread use of these services could accustom the children to be constantly controlled and thus to grow into individuals, who do not consider being monitored as intrusive. Thus, the legitimacy of the processing is doubtful. The law proposal to amend the Electronic Communications Act introduces a specific provision relative to minors above eleven years old, which compels the Operators to obtain their consent before the provision of the service.

The Operator should further offer the subscribers or end users the possibility to withdraw their consent easily, without any charge, definitively or temporarily (Art. 123-4 of the Electronic Communications Act). The modification law proposal extends the obligation compelling the Operator to offer this possibility to both the subscribers and the end users.

However, an exception is foreseen for the needs of provision of emergency services[70]. A Royal Decree, after the Privacy Commission has given its opinion, should specify the procedure according to which Operators should override the temporary or definitive withdrawal of the consent of the user at the request of emergency services willing to answer an emergency call (Art. 123-5 of the Electronic Communications Act). This cancellation is free of charge. This decree has not yet been published.

5.2.4 Limitation of the processing

Besides the obligations stated in the Data Protection Act to controllers (proportionality, finality, data minimisation principle), the Electronic Communications Act has incorporated some of them for the processing of location or traffic data by Telecommunication Operators. According to Article 122-4, the location or traffic data can only be processed and stored for the provision of a location or traffic data based service, respectively. These services are the ones which imply the processing of traffic or location data above those strictly necessary for

[68] Opinion 5/2005 on the use of location data with a view to providing value-added services, WP 115, 25 November 2005.
[69] UNICEF, Convention on the Rights of the Child, 20 November 1989.
[70] These services are defined by Art. 2 of Royal Decree of 2 February 2007 relative to emergency services, M.B. (*Belgian Official Gazette*)13 February 2007, p.7087.

the conveyance of the communication or billing of the service (Art. 2. 8° and 9° Electronic Communications Act).

Moreover, it introduces specific provisions in order to define the persons who can access and process the data. The processing of traffic data, apart from the need of conveyance of a communication, can only be carried out by the persons in charge of the billing process or the traffic management, the processing of the information requests from the clients, the fraud detection, marketing of own services of the Operator or the provision of traffic data based services. However, location data could be processed by any person under the authority of the Operator or the third party which have to provide the location data for the service (Art. 123-4).

5.2.5 Confidentiality and rights of the data subject

Finally, it should be mentioned that, as in processing of any kind of personal data, location data processing should comply with the security measures necessary to guarantee the confidentiality of the processing (Article 16§4 of the Data Protection Act). The Belgian Data Protection Authority has issued ten general principles that every controller should respect in order to comply with the general obligation of confidentiality. [71]

Moreover, the controller should ensure the rights of the individual: right of access, data rectification, and erasure of the data. As already mentioned, the subscriber and the user of a location based service have the right to object to the processing, at any time and without any charge, definitively or temporarily.

5.3 Legal framework for processing location data by public authorities

The processing of location data opens new ways for the public authorities to solve issues related to the general public interest. Some applications are being experimented with in public sectors, notably for traffic management purposes (section 5.3.1). The main processing of location data by public authorities occurs, however, for law enforcement purposes (section 5.3.2).

5.3.1 Innovative Floating Car Data Project

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 specialising in traffic information, a project on Floating Car Data in Flanders[72]. Floating Car Data (FCD) is a method to determine the traffic speed on the road network, which can be realised through the use of several technologies, like CDMA, GSM, UMTS and GPRS[73].

The project was conducted in the region of Antwerp due to the extensive road works that were taking place at the city ringroad at that time. During the validation phase of the project, which

[71] See also: Privacy Commission, Referring Measures in the field of security applicable to every processing of personal data (*Mesures de référencement en matière de sécurité applicable à tout traitement de données à caractère personnel*), available at: <http://www.privacycommission.be/publications.htm>.
[72] Not much information about the Project is available to the public according to the internal agreement of the relevant parties.
[73] <http://en.wikipedia.org/wiki/Floating_Car_Data>.

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 estimated travel time.[74] This technology can be very useful in places where there are no detection loops or cameras, for instance.

The floating vehicle technology (Estimotion)[75] developed by ITIS Holdings plc was used for the gathering the actual data, and these 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 can be obtained after modifying the software, according to ITIS Holdings plc.

Since the collected data – even if a modification of the software is needed for this – can reveal data relative to the origin and the destination of the mobile user, they can be considered as personal data and their processing must follow the principles set out by the Belgian privacy law. The use of location and traffic data for the scope of this project are in fact a secondary processing of personal data and should be based on a legal ground, 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 good. In this case the processing of the data could be based on Art. 5(e) of the Data Protection Act claiming the fulfilment of a task of public interest.[76]

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 should be mentioned that in general the technology was able to detect in a quite accurate way the traffic trends over time per road segment.[77] The data collected during this project are kept in a database and can be used for subsequent traffic analysis.

5.3.2 Processing of location data with purpose of law enforcement

5.3.2.1 Location data in the Criminal Proceedings Code[78]

In the course of the criminal procedure three different measures are foreseen with regard to private communications and telecommunications. The public prosecutor (*procureur des Konings*) has the power to oblige an operator to provide him with the identification data of the regular user of a telecommunications service (Art. 46 Criminal Proceedings Code (*Wetboek van Strafvordering*)). Secondly, article 88*bis* Criminal Proceedings Code contains the

[74] Press release of the Ministry of the Flemish Community on 11 January 2006, available online at: <http://www.mobielvlaanderen.be/persberichten/artikel.php?id=115> (last accessed on 15 December 2006).
[75] Press release of the Ministry of the Flemish Community on 02 September 2004, available online at: <http://www.agoria.be/ICT-TIC-Flash/nl/87/87-10%20pers%20vl%20gem%5B1%5D.doc> (last accessed on 13 December 2006).
[76] Article 5 e) of the Belgian Data Protection Act.
[77] Press release of the Ministry of the Flemish Community on 11 January 2006, available online at: <http://www.mobielvlaanderen.be/persberichten/artikel.php?id=115> (last accessed on 15 December 2006).
[78] Kindt E., Lievens E., Kosta E., Leys T. & De Hert P. 2007. 'Chapter 2: Constitutional Rights and New Technologies in Belgium' in Koops B.J., Leenes R. & De Hert P., Constitutional Rights and New Technologies. A comparative study of Belgium, Canada, France, Germany, Sweden and the United States, Report commissioned by the Dutch Ministry of the Interior and Kingdom Relations, Tilburg, February 2007

procedure according to which the examining magistrate (*onderzoeksrechter*) can oblige operators to provide him with communications data or the data revealing the origin and the destination of a communication (not only location data but also the data revealing the day, time and duration).

Finally, the Belgian legislation allows the eavesdropping, examination, and recording of private communications and telecommunications for the investigation of specific criminal offences. The procedure, which is carried out under the supervision of the examining magistrate, is described in articles 90*ter* until 90*decies* of the Criminal Proceedings Code. These articles specify the criminal offences for the investigation of which the eavesdropping, examination, and recording of private communications and telecommunications can be allowed and describe the procedure to be followed.

5.3.2.2 Data retention[79]

Furthermore, Article 126 of the Electronic Communications Act stipulates that 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. For the enforcement of the obligation of the providers to retain the data a royal decree is currently under preparation and will soon be 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 allowed 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 [*ombudsdienst voor telecommunicatie*] in revealing the identity of people making improper use of electronic communications services or networks.[80] However, it is still too soon to know the exact scope of the data retention obligation, and for instance whether Telecommunication Operators will be compelled to store the location data of a mobile phone in standby mode.

It is worth mentioning that Art. 127 of the Electronic Communications Act allows the King to determine the technical and administrative measures to be imposed on operators or end users, in order to be able to identify the calling line in cases of emergency calls as well as for the investigation of specific crimes. The second paragraph of the article states that the supply or the use of a service or a device that hinders or prevents the aforementioned actions are prohibited. Exception to this rule could be established for encryption systems that can be used to guarantee the confidentiality of communications and the safety of payment. However, such rules have not yet been established by the King, an action that could raise several discussions regarding anonymity.

5.3.2.3 Electronic monitoring of offenders

After being in an experimentation phase since 1996 as a modality of execution of prison term, penal electronic monitoring was extended to prisons throughout the country in July 1999. Ministerial Circular letters have defined the modalities of application of monitoring. The

[79] Kindt E., Lievens E., Kosta E., Leys T. & De Hert, P. 2007. 'Chapter 2: Constitutional Rights and New Technologies in Belgium' in: Koops B.J., Leenes R. & De Hert P., *Constitutional Rights and New Technologies. A comparative study of Belgium, Canada, France, Germany, Sweden and the United States*, Report commissioned by the Dutch Ministry of the Interior and Kingdom Relations, Tilburg, February 2007.
[80] Kosta E. & Valcke P. 2006. Retaining the data retention directive, 22 *Computer Law & Security Report* (2006), p. 370 and p. 377.

penal electronic monitoring procedure has thus been entirely controlled by the Executive power. A Center for Electronic Monitoring has been created in 2000 and is in charge of the monitoring and the following-up of offenders.

This situation has been heavily criticised because of opaqueness and legal uncertainty. This has led to the approval of a specific legal framework in 2006[81], which has created a specific tribunal in charge of the application of sentences (*Tribunal d'application des peines*) and which will deal with the requests of penal electronic monitoring.

Penal electronic monitoring in Belgium is conceived as an alternative to a prison term and can be only accorded to certain offenders:

- offenders in a position to obtain a conditional release after six months,
- offenders sentenced to a total prison term of a maximum of three years, and
- offenders able to support themselves, who have a home and a fixed telephone line.

The offender should request to be placed under electronic monitoring. This is considered as a guarantee of human dignity. Moreover, the consent of the co-habitants is requested.

The actual system of penal monitoring is based on a radio frequency technology. The bracelet of the offender detects whether he stays in the authorised area. More sophisticated systems of monitoring, which would allow controlling an offender through a voice check system, consumption of alcoholised beverages or real time localisation are planned to be introduced. However, because they can be perceived as 'security drifts', a first test period will precede their implementation.[82]

It should be highlighted that there is no specific data protection provision in the law, nor any previous consultation of the Privacy Commission foreseen before the implementation of new methods of penal electronic monitoring. It seems that the legislation relies on the previous request of the offender in order to legitimate the processing of personal data. It follows that the general rules of the Data Protection Act as described above will apply.

Finally, a law proposal[83] introduced after the murder of two girls of 7 and 10 years during the summer 2006 should be mentioned. This proposal suggests the physical implementation of a chip into certain sexual criminals after their release, whereby they are put at the disposal of the government in order to be able to localise them at any moment. A specific committee constituting doctors, psychiatrists and specialised psychologists would control this procedure and such decisions. The justification of this measure into Belgian Law is based on the importance of the early intervention of police services in case of children kidnapping. The proposal concludes that only this technology can ensure enough rapidity of police action, as it enables the localisation of the sexual criminal with the chip present in the perimeter of the attack. Moreover, this measure is presented as facilitating the rehabilitation of the individual

---

[81] Act of 17 May 2006, relative to the external legal status of offenders convicted to prison term and to the rights of the victims in relation to the modalities of execution of the sentence (*Loi relative au statut juridique externe des personnes condamnées à une peine privative de liberté et aux droits reconnus à la victime dans le cadre des modalités d'exécution de la peine*), Act of 17 May 2006 establishing tribunals of application of sentences (*instaurant des tribunaux de l'application des peines*), M.B. 15 June 2006.

[82] Mallié C. 2007. *La mesure de surveillance électroniques en Belgique*, in *Justice et Technologies : Surveillances électronique en Europe*, eds. Froment J.-C and Kaluszynski, PUG and CERDAP, 2007, p.115.

[83] Law proposal relative to the introduction of electronic monitoring and hormonal pharmacological treatment for sexual agressors (*visant à introduire la possibilité de recourir à un dispositif de surveillance électronique et à un traitement pharmacologique hormonal des agresseurs sexuels remis en liberté*), introduced by M. Jacques Brotchi to the Senate, 10 July 2006.

as it is invisible. Once again, no specific data protection provision is included in the proposal in order to asses the concerns raised relative to the right to private life of the individual put under surveillance and of his or her freedom to come and go anonymously.

5.4 Legal framework for processing location data by private parties

Because of the social implications of some location data processing, like the monitoring of employees and children, two law proposals have been passed in order to address to these concerns. Two specific examples will be discussed in this chapter, both with high-growth market expectations: the use of location devices by employers for monitoring of the activity of their employees (section 5.4.1) and the development of C2C (Client to Client) Location Based Services, based on the localisation of a third party's mobile phone (section 5.4.2).

5.4.1 Surveillance of employees

5.4.1.1 Legal provisions applying to these processing

When the processing is realised in the context of a labour relationship, we should refer not only to the Data Protection and Electronic Communications Acts but also to the provisions contained in Labour Law. These relationships are characterised by an imbalance in the power of negotiation of the parties. In Belgium, negotiation and consultation instruments have been used in order to mitigate the consequences of this non-egalitarian relationship (Privacy Commission, Opinion 10/2000[84]).

Nowadays, the employer is getting access to highly intrusive means of surveillance of workers. However, despite the fact that the employer has the power to use communication means and to control the effective implementation and respect by the employees of these rules, he cannot invade the fundamental rights of the employees.[85] The electronic surveillance of workers has been a point of debate for several years in Belgium and a specific collective labour agreement has been set up between trade unions and companies representatives in order to regulate the use of means of control of the data relative to electronic communications networks in 2002[86]. This agreement was meant to define the limits the employer cannot cross without invading the worker's privacy when controlling the activities of the latter in the field of network communications. It particularly focuses on information relative to emails, browsing and chats, but also on data transmitted by mobile phones.

The processing of location data for purposes of control over the activities of the worker and improvement of the work organisation motivated the presentation of a Law proposal[87] that is

[84] Opinion nº10/2000, Opinion relative to the surveillance by the employer of the use of informatics system at workspace (*Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail*), 3 April 2000.
[85] Arts. 2,3,16,17 of Law of 3 July 1978 relative to working contracts recognise to the employer the right to control and organise the working activity and Article 22 of the Belgian Constitution recognises every individual the right to privacy.
[86] Labour Collective Agreement nº81 of 26 April 2002 relative to the protection of workers' private life with regard to the control of data in electronic communication network (*relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électronique en réseau*).
[87] Law proposal relative to the surveillance of workers by monitoring systems based on GPS systems in professional vehicles according to the provisions of the Data Protection Act (*visant à encadrer la surveillance*

currently discussed at the Senate. The law proposal aims at the setting up of a new Collective Labour Agreement relative to the control of employees with the purpose of controlling the professional use of companies' vehicles and the correct application of the conditions of work.

Until the final approval of the law and the setting up of a new agreement, several laws apply to such data processing:

- The *Data Protection Act* regulates the obligations and rights of the controller (the employer) and the data subjects (the employees),
- The *Electronic Communications Act* regulates the obligations and rights of the Operator and of the subscriber of the service (the employer) and the users (the employees),
- The *Collective Labour Agreements* nº 13[88], 39[89] and 81[90] establish the general principles that should be respected in case of electronic surveillance of workers, even if it does not specifically refer to location data processing. A reference shall be also made at this point to the Opinion of the Privacy Commission on the Law Proposal relative to the surveillance of workers by monitoring systems based on GPS systems in professional vehicles according to the provisions of the Data Protection Act, as it contains the general principles, which should apply to such processing in the field of data protection.[91]

Data Protection Act

The employer is the natural or legal person who determines the purposes and means of the processing of personal data, and thus is considered as controller of the processing. He has the obligation of obtaining the prior consent of the worker and to provide him with the relevant information as stated by Art. 1.4 of the Data Protection Act. It should be mentioned that the consent of the trade unions through a General Labour Agreement can not be a substitute for the individual, free, specific and informed consent of the worker to the processing.[92]

When the processing is intended for surveillance purposes, the information provided to the workers should contain the information stated in Art. 9 of the Data Protection Act (name and

---

des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée).

[88] Collective Labour Agreement n° 13 bis of 26 February 1979 adjusting collective Labour Agreement to the Act of 3 July 1978 relative to working contracts (*adaptant à la loi du 3 juillet 1978 relative aux contrats de travail, la convention collective de travail n° 13 du 28 juin 1973*), as modified by collective labour agreement nº 13 ter of 1 February 1983, 13 quarter of 6 December 1983, 13 quinquies of 16 December 1986 and 13 sexties of 28 July 1992, ratified by Royal Decrees of 23 March 1979m 7 April 1983, 8 February 1984, 29 January 1987 and 22 October 1992, published at MB of 24 April 1979, 26 April 1979, 26 April 1979, 26 April 1983, 22 February 1984, 11 February 1987 and 13 November 1992.

[89] Collective Labour Agreement n° 39 of 13 December 1983 relative to information and consultation on social consequences of the introduction of new technologies (*concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies*), ratified by the Royal Decree of 25 January 1984, M.B. of 8 February 1984.

[90] Collective Labour Agreement n° 81, relative to the protection of worker's privacy with regard to the control of electronic communications in a network (*relative a la protection de la vie privee des travailleurs a l'egard du controle des donnees de communication electroniques en reseau*), 26 April 2002.

[91] Privacy Commission, Opinion on Law proposal relative to the surveillance of workers by monitoring systems based on GPS systems in professional vehicles according to the provisions of the Data Protection Act (*visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée*), 7 September 2005.

[92] Opinion of 7 September 2005, op. cit.

address of the controller and, if such is the case, of his representative; the purposes of the processing; recipients or categories of recipients of the data; the existence of the right of access to and the right to rectify the personal data concerning him), how the control is realised, the nature of abuse which can lead to a control, the duration of the control and the procedure followed after the control (Art.9 Collective Labour Agreement n°81).

The processing should have defined, explicit and legitimate purposes, i.e., it should be linked and justified by the activity of the employer. In the context of the control exercised by the employer on the working tools, the Privacy Commission reminded in its Opinion 10/2000[93] that the definition of what is allowed or not in the workspace will depend on several factors, as the work context, the nature of the responsibilities of the employer and the employee, and the nature of the work in itself. This issue should be treated on a case-by-case basis into each company. This statement will be equally valid for the processing of location data by the employer.

For processing of location data with purpose of control of workers, the Privacy Commission recommended that the Labour Convention defines the purposes of the surveillance, mentioning some criteria as for instance the security of the worker, the protection of the vehicle, to the existence of professional needs regarding transport and logistic or the control the employees' work. [94]

The processing should also be proportionate. A proportionality test should be carried out in order to balance the interest of the employer and the respect of fundamental rights of the employees. Art. 6 of the Labour Collective Convention nº81 set up a general principle, according to which the control of the information flow in the communication network should not imply an invasion to the privacy of the worker. The processing of location data of the worker will not only risk violating the worker's privacy but also his freedom of movement in an anonymous way. Therefore, the employer should ensure that the system does not constitute a disproportionate intrusion into these two fundamental rights of the worker. This means that he cannot implement such a system with the sole purpose to control the movements of the employer. Moreover, the data minimisation principle compels the controller to process only adequate, relevant and not excessive personal data regarding the purposes of the processing. The Privacy Commission considers that in case the system is implemented for the control of the tasks, such control could only be justified occasionally and on the basis of hints, which indicate the abuse from some workers. A permanent control and processing should be considered as disproportionate and it reminds that the best solution would be to allow the worker to activate and deactivate the system according to the needs of the localisation, as well as outside working hours. [95]

Moreover, the controller will have to ensure the confidentiality of the processing and set up the required security measures, as well as attending the request of access, modification and cancellation formulated by the data subject (the worker). The worker has a right to object to the processing whenever he has serious and legitimate reasons (Art. 12 of the Data Protection Act).

Electronic Communications Act

[93] Op. cit.
[94] Opinion of 9 September 2005, op. cit.
[95] Opinion of 9 September 2005, op. cit.

The Electronic Communications Act provides that the Mobile Operators shall obtain the prior consent of the subscriber to the location based service (the employer) and when appropriate of the user (the worker). Moreover, as mentioned above, the Telecommunication Operator should enable a system allowing the easy deactivation of the processing, at any moment and without charge. The approval of the proposal of law modification would mean that the Operator will have to obtain, in any case, the consent of both the employer and the worker prior to the activation of the system.

Labour Law

As highlighted by the Privacy Commission in its Opinion nº10/2000, the labour legislation as a whole established a general principle according to which employers should inform and consult their employees or their representative prior to the introduction or modification of automatic systems with purposes of gathering and using workers' personal data. This principle also applies to the introduction or modification of technical processes intended to control workers' movements or productivity.

Article 2 §1 of Labour Convention No. 39 of 13 of December 1983, relative to the information and consultation on the social consequences of the introduction of new technologies, states that when the employer decides to invest in a new technology, which has important collective consequences regarding the employment, the working organisation or the working conditions, he has to provide written information on the nature of the new technology, the factors which justified its introduction and of the social consequences and to lead a consultation with workers' representatives on such social consequences, at the latest three months after the implementation of this new technology.

Finally, Article 6 of the Law of 8 April 1965 on Work Regulations states that these regulations have to indicate the right and obligations of surveillance staff. This article has constituted the legal basis of Labour Convention nº68 relative to the protection of workers' privacy regarding video surveillance in the workspace.

The Collective Labour Agreement nº81 applies to communication data in a network, understood in a broad meaning and irrespective of the support by which they are transmitted and received by a worker in the frame of a work relationship. It follows that the surveillance through a monitoring system linked to a GPS navigation system in a professional vehicle used by employees can only be implemented after the agreement of *ad hoc* joint commissions, the Public services common committee or competent bodies.

5.4.1.2 The example of GeoMobile's Location Based Services

GeoMobile is a service offered in Belgium by the company 'NETiKA Internet & Mobile Solutions'.[96] This service enables the localisation of vehicles or employees. The localisation can take place either via GPS (through a satellite network) or via cell phones (as a Location Based Service). The latter service is currently offered in co-operation with two mobile operators, Proximus and Mobistar.

The localisation can be visualised in real time on a card that is shown on the screen of the employer's computer and the system allows the simultaneous localisation of more than one vehicle or employee. The service is equipped with a multitude of extra functions, such as the

[96] See <http://www.geomobile.be>.

calculation of the estimated time till reaching the target address, grouping of the employees and the interactive communication between the employer and the employee via SMS or e-mail[97].

GeoMobile compels the person who uses its services to inform the mobile workers about the localisation system and its purposes and obtain their prior consent to be localised. The two should also agree on the hours during which the localisation is going to take place, before the actual activation of the service. For the cell phone service the employee has to send an SMS to the operator and, in both cases, he has to sign a form, a model of which is provided on the Website.

For the provision of the service, both via GPS and via cell phone, location data of the employee are used and therefore the consent of the person who is going to be localised is needed. It is important to mention that the employer is the one who has to give to the employee the necessary information about the service.

5.4.2 Localisation of third parties' mobile phone: Ootay

In 2005, the first C2C (client to client) location based service, called Ootay, emerged in Belgium. This service allows the identification of the base station to which the user's mobile phone is connected, using a Cell-ID system. The accuracy is thus variable depending on the density of base stations: in city areas, the average accuracy is from 100 to 300 meters, although in rural areas it can go to as much as 30 kilometers.[98] The person who makes the request receives a map where the mobile phone, whose localisation was asked, is actually located.

This service situates itself in the emerging market of "child locating" which was expected to yield 220M€ in 2006 for Europe. Nowadays, children have gained important autonomy because of changes in society (parents who both work, trips for holidays, sports, etc.). But this service allows not only the localisation of children but also of elderly people, friends or even one's own mobile phone. This service is expected to have important applications with regard to the localisation of elderly people, especially Alzheimer or dementia patients.

The company in charge of its development has implemented a series of security measures in order to prevent fraud and unwanted localisation. First, the verification of the identity of the requesters is based on a process of authentication through their mobile phones. Then, a request of localisation is sent to the third party with a random delay in order to prevent mobile phone theft. The third party should agree by a "validation" SMS for the localisation to take place. After the localisation, a SMS is sent to the localised person in order to remind him the contact details of the person who made the request. Moreover, the third party can deactivate the possibility of being localised by sending an SMS with the text "stop". All the software architecture is secured (firewalls, routers filters, etc.)

5.5 Institute for BroadBand Technology (IBBT) in Flanders

The interdisciplinary Institute for BroadBand Technology (IBBT) is a research institute founded by the Flemish Government, focusing on information and communication technology in general and applications of broadband technology in particular[99]. IBBT consists of initially

[97] Most likely to the PDA of the employee.
[98] See section 3.2.
[99] <http://www.ibbt.be>.

14 participating research groups focusing not only on the technical but also on the legal and social aspects of information and communication technologies. IBBT is promoting research with more than 30 ongoing projects mainly focusing on eGovernment, eHealth, new media, mobility and enabling technologies[100].

Below we will briefly present some of the projects where location data are in the centre of research for several applications.

Crisis management is often needed for mastering disasters, e.g. a major fire in industrial or chemical environments. The major challenge in such a crisis is to provide the authorities with concise and exact information in real-time through a crisis management system. Such a system should process dynamic data collected through a mobile network, and present the derived information together with information that has a static nature, in combination with geographical information. That is the system that will be studied, implemented and demonstrated in the *GeoBIPS* (Geographical Broadband Integration for Public Services) project. Hence, the overall goal of this project is to specify, design and build a demonstrator of a system that collects, processes, displays and distributes static and dynamic information on top of a geographical information system (GIS), using wireless broadband technology with an application to a crisis intervention system that provides a real-time overview of the disaster area for a fire department..

The end-goal of the project *SPAMM* (Solutions Platform for Advanced Mobile Mesh) is to specify, to research and to design a demonstrator of a mobile platform (targeted towards cars, buses, trucks etc.) which, through different networks, always keeps the best possible connection between both the vehicle and its backend infrastructure and between vehicles themselves (*ad-hoc* or mesh networking[101]). The innovation inside the networking part of the project can be found in the dynamic switching between different networking modes. If a vehicle is connected through a public hotspot and moves out of range of this hotspot, there has to be a way to switch to *ad-hoc* networking to connect to the back-end infrastructure through other hops. If there are no other peers available to form a connection to the back-end, the platform must connect to the best available narrowband network (GPRS or UMTS). The convergence between the different networks needs to happen in a transparent manner for the user, without requiring any form of action on his/her part. The dynamic switching between the network modes also needs to happen with as little data loss and delay as possible.

The aim of Architectures for Mobile Community Content Creation (*A4MC3*) is to explore the possibilities of community building using advanced technology - mobile terminals, wireless networks, multimedia and metadata technology - to create a virtual online community for the residents of a Belgian city. A multi functional mobile device (e.g. PDA) which is connected to a metropolitan wireless network and is distributed to the residents, acts simultaneously as a publishing tool (through which the residents can 'feed' user created content to an online database) and a receiver of location based information. In the said case, different user groups are targeted: the average end-user (someone in the street who uses his digital camera to capture content and upload it to the online database, or comments on the food quality of a specific restaurant), the advertiser (who is trying to reach the consumer in a targeted way, by

[100] A full list of the projects can be found at: <http://www.ibbt.be/site/index.php?id=124&L=1>.
[101] Mesh networking is a way to route data, voice and instructions between nodes, allowing for continuous connections and reconfiguration around broken or blocked paths by "hopping" from node to node until the destination is reached. See <http://en.wikipedia.org/wiki/Mesh_networking>.

offering location based information), the professional journalist (who is reporting from a specific location) and the moderator of the virtual community (as the intermediary engaged in the provision of the online service).

Wireless technology is a key driver in adding value in building automation through the deployment of technology. Indeed, installing and commissioning a myriad of wired networks has been reported to be a major source of effort and thus of cost. The multitude of wired networks in a typical professional building consists of the computer network, the fire alarm network, the emergency lighting network, the access control network, etc. Recently the different networks are being deployed using a building automation bus system such as EIB, LON and BACNET. Where the interoperability issues for these wired networks are gradually being solved, fundamental technological problems remain when deploying these services over wireless networks. The *WBA* (Wireless Building Automation) project hopes to redefine the state of the art in wireless building automation, facing challenges like how it would be possible to implement new functionality such as indoor positioning, by reusing the wireless technology infrastructure used for the wireless networks deployed for other tasks.

The Goal of *ADAMO* (Advanced Disaster Architecture with Mobility Optimizations) project is to specify, research and develop a demonstrator for disaster control architecture where persons on the disaster site and persons in the crisis centre are provided with a real-time view on the complete scope of a disaster. ADAMO will provide every link in the information chain through constant and specific updates of the existing information.

The project *FLEXSYS* (*Flexibel verkeersbeheersysteem:* flexible traffic management system) aims at the dynamic adaptation of traffic management systems to the ever-changing road circumstances, like road works, traffic diversions, emergency clearances etc. For that purpose the project researchers must conduct important innovative interventions in the different links of a traffic management value chain: detection, network and communication, data processing and signalisation.

5.6 Conclusion

Location data processing is subject in Belgium to two different frameworks: the Data Protection Act and the Electronic Communications Act. The latter will only apply to the processing of location data obtained from a public electronic network. However, the spread of Location Based Services based on the localisation of third party's mobile phones have raised other issues apart from the strict privacy-related ones and could have important social consequences that the legislator should not avoid to deal with. Two law proposals are currently in the process to be enacted in order to give a solution and to increase the protection of the user against misuses of these services. The option taken for the regulation by collective labour agreements relative to the monitoring of employees through localisation devices is particularly interesting although it is part of a long tradition of negotiation.

On the other hand, new applications, whose development is led by Public Authorities, are emerging in order to solve general societal problems such as the regulation of vehicles traffic in big cities. Although theses new services are still in a phase of experimentation, they start raising new issues regarding the protection of the rights of the citizen either to privacy or to freedom of movement in an anonymous way and their balance with incoming new public interests. This situation could lead to providing Public Authorities with increased amount of information with the correlated risk of re-use of this information for other purposes.

6 Location Information from a French Perspective

Fanny Coudert (ICRI)

6.1 Introduction

During the last few years, increasing location data processing with mainly commercial purposes has raised new concerns in the data protection field. Not only is the right to privacy at stake but also the freedom of movement in an anonymous way.

The enhancement of Location Based Services technologies through the development of electronic communications technologies, as for instance the use of triangulation techniques which combine GPS with GSM, as well as the drop in costs, have made Location Based Services more affordable and accessible to a large audience. Also, the development of smart cards has fostered their use in commercial applications, as for instance through the implementation of e-tickets for public transport. As a consequence, these services have spread and the French Data Protection Authority, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), is receiving each day more complaints and applications for consultations regarding the processing of location data. This has led the CNIL to initiate a reflection on these new issues, through its successive opinions.

Before describing the existing legal framework in France, a definition of location data needs to be provided. French legislation only provides a definition of location data in the context of electronic communications where it means "data allowing the localisation of the user's terminal equipment" (Art. L.34-1.IV of the Post and Electronic Communications Code). As a consequence, the location data will always refer to terminal equipments which should be linked to their owner (the subscriber) or their user in order to get their location: the localisation of the individual is thus indirect, except in the case where the device is embedded in the human body, like an RFID chip. However, this definition does not specify which kind of data it refers to. We should look at Directive 2002/58/EC in order to obtain a more precise definition. Recital 14 of the Directive states that location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded. It thus includes a large range of data which are able to provide a vast amount of information relative to the position and movements of the user.

Out of the context of public networks of electronic communications, location data will refer to the data indicating where a person is at a certain moment. These data can originate from the use of smart cards as in the case of e-ticket applications, but also from private networks of communications or from taking pictures by traffic control devices.

The nature of the Location Based Services provided through public electronic communications networks has evolved from services focused on the provision of information to the individual, e.g. finding the closest restaurant or chemist to the position of the user either through GPS or GSM, to most sophisticated services based on a continuous use of location data, e.g. navigational assistance. Nowadays, the type of services offered has moved one step forward allowing the localisation of individuals not only at their own request but also on request of third parties (WP29, WP115: 4). As a consequence, the nature of these services has moved from localisation actively requested to localisation passively experienced (Gasse D., 2005 CNIL Annual Report: 45). From the perspective of data protection rules, the key issue

has moved from the need to define the conditions in which data shall be stored, to the concern of the legitimacy of the processing (WP29, WP115:4).

The first generation of Location Based Services, based on the previous request of the user, has developed in France principally for the purposes of vehicle localisation, gaming and information services. In the first case, the location can be required either for the provision of assistance to drivers in case of emergency (accident, breakdown, malaise, etc.) or theft. The device can be activated manually or automatically after a crash or a call from the owner informing that his car had been stolen.

The second generation of services offered allows the subscriber to locate the device on demand, even if the device is used by a third person. This kind of service presents higher risks with regard to fundamental rights as it empowers the subscriber to localise the user upon request. In France, this evolution is raising several concerns, not only regarding privacy but also with regard to the freedom of movement in an anonymous way. In the field of privacy, a definition of the limits between the right to privacy and other competing interests, as for instance the right of the employer to control his employees and to organise the company, needs to be found. Regarding the freedom of movement in an anonymous way, safeguards need to be implemented, as long as these new technologies and services could place the individual under constant surveillance. This appears especially worrying in the field of the surveillance of children by parents as it could lead the children to get used to being tracked and watched. The application and interpretation of data protection rules will play a key role in defining the level of intrusion and surveillance tolerated, with regards to these fundamental rights.

In this category, we can find, for instance, services of "free" localisation of the vehicle, which enable the owner to know every moment where his car is, the itinerary followed, the speed, etc. Employers can use these services in order to control the use of the car by the employee, with the purpose of improving costs, the organisation, or the effective working hours of its employees. Insurance companies intended to implement this processing in order to control the driver's behaviour, offering in compensation a reduction of the policy rate.[102] Finally, it is important to mention the development of the location systems of GSM and other mobile devices used mainly either by groups of friends in order to localise each other, or by parents to watch out for their children.

The use of Location Based Services is expected to evolve towards the development of technologies supporting the services. The use of Internet tools in relation to GPS and GSM devices will open a new field of business possibilities. The spread of WiFi access points will open the way to services that allow sending to the user adequate and relevant content according to his position. Marketing can find a new life in the development of Location Based Services, e.g., storekeepers will be able to send customised offers to the subscribers located in the shop area. On the other hand, the electronic bracelet is being implemented, not only for safety purposes, for the resocialisation of offenders, or as an alternative to overpopulated jails, but also for medical purposes, e.g. for the surveillance of Alzheimer patients. Some areas are defined in order to warn the subscriber, usually through SMS, when the user enters them. These bracelets are already sold in drug stores and in the sales points of the Telecommunication providers.

[102] CNIL refused to authorise this kind of processing because it appeared disproportionate. See below, 6.4.2.

The first sections below will be dedicated to the general legal framework applying to location data processing, either for the processing of these data by public authorities or by private bodies. The following chapter will present the main processing of location data in France, both in the Public and the private sector, and how a balance has been found in each case. This will give a general overview of how the privacy right and the freedom of movement in an anonymous way are protected against the implementation of intrusive location data processing.

6.2 Legal framework: general principles

All personal data processing should comply with the provisions of the Data Protection Act. [103] However, when the location data are originated from a public electronic communications network,[104] supplementary safeguards have been introduced by Article L.34-1 of the Posts and Electronic Communications Code, which transposes Directive 2002/58/EC. These safeguards are mainly focused on the consent and information of the subscriber and the user of the service.

These rules, in the context of processing of location data, will not only protect the privacy of the user but also the freedom of movement in an anonymous way. However, they set up a series of principles that remain formulated in broad terms. Their modalities of application will be defined by the CNIL and the jurisprudence, which have the difficult task to find a balance between the compelling interests of each situation.

The CNIL is defining a set of specific rules for the processing of location data through its opinions. It distinguishes depending on the purposes: the guarantees required will not be the same in the context of the data processing related to private or professional life[105]. The CNIL is thus drawing the thin line that processing should not cross in order to remain compliant with the legislation and "fundamental-right friendly".

In this chapter we will describe how French legislation applies to location data processing. In each case, we will first explain the general rule applying to all processing of location data, and when appropriate, specify the particular rules established by the Code of Posts and Electronic Communications. The principles have been divided in three main groups: principles related to data quality (1), consent (2), and confidentiality and rights of data subjects (3).

6.2.1 Data quality

6.2.1.1 Purpose specification, purpose limitation and proportionality

The French Data Protection Act requires the data to be obtained for specified, explicit and legitimate purposes, and subsequently not to be processed in a manner that is not compatible with those purposes (Article 6). The legitimacy and thus the proportionality, i.e. whether the use of location data is proportionate to the objectives foreseen, of the purposes should be evaluated depending on the nature of the activity of the controller, or of its competences if it is a Public Authority. Besides, the gradual use of data for purposes other than those for which

[103] Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties.
[104] According to Art. L.32.3°, a public electronic communications network refers to networks established or used for the provinding of publicly available electronic communications services.
[105] Grasse D. 2006. *Proteccion de los datos personales y geolocalizacion*, datospersonales.org, n°21, 3 May 2006.

it was collected (commonly known as function creep) is criminally punished by reclusion and by a fine up to 300,000 euros[106].

This principle poses a first limit to the expansion of location data processing, as long as the processing will need to find a justification in the activity developed by the controller. Taking into consideration the highly-intrusive nature of location based processing into privacy and the freedom of movement in an anonymous way, especially when they serve the purpose of locating third parties, the CNIL will verify that the processing is really necessary regarding the purpose and that it can not be reached by other means less intrusive or more "fundamental rights-friendly". For instance, the High District Court of Paris annulled the authorisation given for the processing of biometric data for purposes of controlling the employee's working hours. This technique could not be justified by the need to control working hours, as long as a badge system could be as efficient as the one based on biometric data.[107] This example illustrates that the concept of finality works in French Law as a basic guide-rail with regard to the protection of fundamental liberties and rights.

6.2.1.2 Data minimisation principle

The data to be processed should be adequate, relevant and not excessive in relation with the purpose of the processing (Article 6-3° of the Data Protection Act). The data minimisation principle acts here as a second barrier in order to limit the collection of data which would not be strictly necessary for the provision of the service. The processing of location data could lead to the archiving of every user's movements, providing an important source of information for profiling and an important risk for individual liberties. This principle will play an important role in the definition of which location data appear necessary for the provision of the service.

6.2.1.3 Conservation of the data

Finally, the data should not be stored for a period longer than it is strictly necessary for the purposes for which they were obtained and processed. These periods will usually be linked to a limitation-of-legal-proceeding period issued from the processing, i.e., the period during which the liability of the controller can be challenged. However, this principle is strictly applied and should be explicitly grounded on a legal provision. For instance, when location data are processed for the provision of a location based service by a Telecommunication Operator, they can be stored up to one year, the period during which the user can contest the invoice. After this period, the location data should be automatically deleted or made anonymous.

---

[106] Article 226-21 of Penal Code stipulates that: "Anyone holding personal data at the time of its recording, classification, transmission or any other form of processing who diverts this information from its proper purpose, as defined by the legislative provision or regulation or decision of the National Commission for Data-processing and Civil Liberties authorising automated processing, or by the preliminary statement made before the implementation of such processing, is punished by five years' imprisonment and a fine of €300,000."

[107] Tribunal de Grande Instance de Paris, 19 April 2005, not published. A sum up of the content is available at: <http://www.cnil.fr/index.php?id=1824&news[uid]=257&cHash=7048e700be>.

6.2.2 Consent

6.2.2.1 Prior consent

The Data Protection Act admits several grounds for the processing of personal data. The main one will rely on the consent of the data subject (article 7). However, Art. 7 admits derogation to this principle and for instance, the processing can be run without the consent of the data subject when the processing is based on the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject. This ground will play a significant role for the monitoring of employees. This means for instance that the location data processing of the employee's vehicle does not require, for its legitimacy, the previous consent of the worker, whenever it responds to a legitimate interest of the employer, and is compatible with the freedoms and liberties of the employee. The difficult interpretation of this provision is realised by the CNIL.[108]

As mentioned above, when location data are originated within a public network of electronic communications, Article L.34-1 of the Posts and Electronic Communications Code requires Telecommunication Operator to obtain the prior consent of the subscriber for the processing. Operators which foresee to offer their own services on the basis of traffic data should obtain his express consent. In the later case, the consent can only be given for a limited period which can not exceed the one required for the provision or marketing of the service.

Art. L34-1.IV of the Post and Electronic Communication Code introduces an exception to this rule, relative to emergency calls in order to facilitate the provision of assistance. In this case, the mere fact of calling an emergency service implies to consent to the processing of the location data. The consent will be valid until the end of the assistance or rescue operation and with this sole purpose.

6.2.2.2 Information provision

In order for the consent to be valid, it should be informed. Despite the fact that the French Data Protection Act does not provide a definition of "consent", it introduces the obligation of prior information to the processing which will play a key role in the validity of the consent given, as it guarantees an enlightened, free and specific consent. Art. 32 of the Data Protection Act compels the controller to inform the data subjects of its identity, of the purposes of the processing, whether replies to the questions are compulsory or optional, the possible consequences for him of the absence of a reply, the recipients or categories of recipients of the data, its rights of access, rectification, deletion and objection, when applicable, the intended transfer of personal data to State that is not a Member State of the European Community.

Article L.34-1.IV of the Posts and Communication Code set up a specific rule regarding the information to be provided. The subscriber should be informed before the processing of the data processed, the duration and purpose of the processing, and of the transfers of the data to

[108] Decision n°2006-066 of 16 March 2006 adopting a recomendation relative to the implementation of employees of a public and private bodies vehicles' localisation devices (*portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public*), J.O n° 103 du 3 mai 2006.

third party service providers. This information should also be provided to the user in order to enable him to exercise his right to object to the localisation.

6.2.2.3 Right to object

Article 38 of the Data Protection Act acknowledges a right to object to the data subject. This right is conditioned to the existence of legitimate reasons, unless where the processing satisfies a legal obligation or where an explicit provision of the decision that authorises the processing excludes the application of these provisions. The controller is entitled to evaluate the legitimacy of the request and to deny it. In case of denial, the competent Court will resolve the legal dispute.

Article L.34-1.IV of the Post and Electronic Communication Code provides the subscriber with a right to object to the processing of their location data, at any time and free of cost (except from the costs linked to the communication of the withdrawal, e.g. the cost of the SMS), without having to justify their withdrawal. This article also acknowledges a specific right to the user of the service, when he is a different person from the subscriber, to suspend the consent given by the subscriber, i.e. to deactivate the localisation device.

6.2.3 Confidentiality and rights of the data subject

Finally, it should be mentioned that, as in processing of any kind of personal data, location data processing should comply with the security measures in order to guarantee the confidentiality of the processing (Article 34 of the Data protection Act). These measures should be both physical and logical and should be adapted to the nature of the data processed and to the risks offered by the processing. The infringement of this provision is punished by up to 5 years in prison and a fine of up to 300,000 euros (Art. 226-17 of the Penal Code).

Moreover, the controller should ensure the respect of the rights of the individual: right of access, of rectification and of erasing of the data. As already mentioned, the subscriber and the user of a Location Based Service have special rights to object to the processing at any time and free of cost (except from the costs linked to the communication of the withdrawal, e.g. the cost of the SMS).

6.3 Legal framework for processing location data by public authorities

The French Data Protection Act applies to all controllers whether they are Public Authorities or companies from the Private sector. Therefore, the processing of location data by public agencies or public companies will have to comply with the data protection principles described above. The sole exception consists in the process of authorisation by the CNIL of some specific processing. Article 26 stipulates that an order of a competent Minister or Ministers shall authorise, after a reasoned and published opinion of the CNIL, the processing of personal data carried out on behalf of the State and which involves State security, defence or public safety; or whose purpose is the prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of criminal sentences or security measures. In these cases, the opinion of the CNIL shall be published together with the order authorising the processing, but it is not binding.

Regarding the provisions of Art. L.34-1 of the Code of Posts and Electronic Communications, they will apply whenever the data originate from a public electronic communication network.

This chapter will first focus on three examples of processing of location data by Public Authorities, before describing the rules applying to the requests and use of location data by Public Authorities for law enforcement purposes.

6.3.1 Processing of location data by public authorities: examples

Three examples of processing of location data that present great interest are going to be analysed in order to illustrate the main purposes which Public Authorities use them for: the use of e-tickets in public transport which leads to the collection of location data with commercial purposes but also with purposes of control and repression of fraud, the taking of automatic picture of cars when their drivers infringe the Traffic Code and the use of e-bracelets for offenders. None of these examples imply the use of a public network of communications and thus Art. L.34.1 of the Code of Posts and Electronic Communications will not be applicable.

6.3.1.1 Use of e-tickets in public transport

Public transport companies, through their modernisation process, have started to offer to their users magnetic, chip or RFID cards in order to ease their movements into the network and to offer them complementary services. Users do not have to buy and carry a paper-ticket any more. However, as these devices memorise more data than that strictly needed for the provision of the service, data protection issues have been raised. They not only allow the user to use the public transportation network but also record the itineraries of the users collecting the time, data and place of entrances, exits and interconnections. This situation raised specific issues of proportionality of data collected, legitimacy of the processing and of the period of storage of these data.

In 2003, the CNIL issued a recommendation which defines the case where public companies were entitled to proceed with such processing and how long they could store the data collected.[109] The only purposes considered as legitimate are the ones relative to the management of subscription rates, commercial relationship, statistic analysis and measurement of the quality of the system and fraud control. The personal data collected through e-tickets cannot be processed for any other purposes.

Moreover, the CNIL advocates for the anonymisation of the personal data in order to guarantee the freedom of movement in an anonymous way ensured by the use of a paper-ticket. The data should not be stored for a period exceeding two successive days and in the case of data gathered as the consequence of fraud detection, they should not be stored more than the necessary time to verify the reality of the fraud, and to enable the examination of the case by judicial authorities.

6.3.1.2 Automatic taking of car pictures for repressing traffic offences

The Act of 12 June 2003 reinforcing the fight against traffic violence[110] foresees that a fine notice can be sent as a consequence of the recognition of an infringement of the traffic code

[109] Resolution n°03-308 of 16 September 2003 relative to the adoption of a recommendation on the collection and processing of personal data by public transport companies in the context of ticket uses (*portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives par les sociétés de transport collectifs dans le cadre d'applications billetiques*), J.O. n° 255 of 4 November 2003, p. 18786.
[110] Law n° 2003-495 of 12 June 2003 strengthening fight against road violence (*renforçant la lutte contre la violence routière*), J.O. of 13 June 2003.

made by automatic means. This provision mainly raised the problem of its compatibility with the previous article 2 of the Data Protection Act which forbid a decision with judicial consequences to be taken on the basis of automatic process. But it also raised the problem of the processing of location data, as long as the processing reveals the location of an individual at a precise moment. Even if the purpose of the processing remains to control the vehicles and not the individuals, they create a feeling of being under constant surveillance and thus raise data protection issues (CNIL). Especially if we take into account that in this case, the previous consent of the driver is not required, as the processing is carried out for the purpose of repression of offences.

However, the CNIL considered that even if the consent of the driver was not required in this case, he should be informed when he receives the fine of the existence and purposes of the processing, the identity of the controller, its rights of access, rectification and. Especially when a specific period of data retention of ten years was established by article L121-3 of Traffic Code.

In 2003, the CNIL gave a first positive opinion on an experimentation conducted by the Ministry of Internal Affairs which intended to implement the automatic taking of pictures of the cars and their passenger when they infringe the speed limits.

The personal data processing included not only the driver and passengers of the vehicle but also the data relative to the offence, such as place and date of the infringement. This processing allows the defining of the location of an individual in a specific moment.

In October 2004, this system has been fully approved by the CNIL and extended to other traffic offences foreseen by Art. L.121-3 of the Traffic Code: respect of security distance between vehicles, the failure to follow stop signs, non payment of tolls fees and the forbidden presence of a vehicle in specific roads or on the pavement. It will apply not only to the French but also to foreign drivers.

6.3.1.3 Electronic bracelet for offenders

Since 2002, several provisions have been introduced into the Criminal Procedure Code for the electronic surveillance of convicts in the context of a diversification of alternative measures to prosecution, incarceration, and to the ones pronounced during the application of the prison term[111]. Particularly, the Act of 12 December 2005 on repetition of penal offences treatment[112] introduced into French Law the possibility of putting convicts under mobile electronic surveillance after their release, when their dangerousness has been certified, whenever they consent to it. The Public agency in charge of the processing will be able to know where the convict is at every moment and thus, despite being an alternative to prison, its highly intrusive nature does not allow the State to compel the convicts to opt for this kind

[111] Decree n° 2002-479 of 3 April 2002 modifying the Criminal Procedure Code and relative to electronic surveillance (*portant modification du code de procédure pénale (deuxième partie : Décrets en Conseil d'Etat) et relatif au placement sous surveillance électronique*), J.O. n° 84 of 10 April 2002 p. 6322; Law n° 2004-204 adjusting justice to the evolutions of criminality (named “Perben Act II”) (*portant adaptation de la justice aux évolutions de la criminalité (dite "loi PERBEN II")*), J.O. 10 March 2004; Decree n° 2004-243 of 17 March 2004 relative to electronic surveillance and modifying the Criminal procedure Code (*relatif au placement sous surveillance électronique et modifiant le code de procédure pénale (deuxième partie : Décrets en Conseil d'Etat)*), J.O. n° 68 du 20 mars 2004 p. 5396.

[112] Act on repetition offences treatment (*Loi relative au traitement de la récidive des infractions pénales*), J.O. of 13 December 2005.

of reclusion. The processing will be legitimate on the basis of the consent given by the convict and the processing should be limited to the personal data strictly necessary for the surveillance. The fact that consent was required was one basis of the constitutional validation of the measure by the Constitutional Council. [113]

This processing knows the location of the persons wearing e-bracelets through GPS or GSM techniques. The electronic bracelet informs the location of the convict each 30 seconds, and warns through SMS the competent authorities when he is out of the "security area". A law proposition is in debate in the National Assembly regarding the electronic surveillance of convicts aged 70 years and older.

This Act allows the use of an e-bracelet for a period of two years, renewable once or twice, in defined cases:

- in the case of socio-judicial follow up of individuals above 18 years convicted to an at least 7-year prison term and whose dangerousness has been certified by a medical expertise
- as a modality of execution of the punishment (conditional release)
- as a measure of judicial surveillance ordered against individuals convicted to prison terms over 10 years for specific crimes

The CNIL opinion[114] reiterates that the processing should respect and guarantee the human dignity, integrity and privacy of the individuals, as well as encourage social reintegration. Regarding these purposes, some data, at first foreseen to be collected, have been abandoned, such as the name of the relatives of the convict, following the opinion of the CNIL which considered their collection disproportionate with regard to the finality of the processing. It highlights the importance of obtaining the consent of the individual, which should be obtained through a debate organised by the magistrate. The information provided to the convicts before they volunteer to the experimentation has been revised by the CNIL as well. Moreover, a specific reference is made to the modalities in the exercising of the right of access, which should be guaranteed in any case.

Other considerations are taken into account as well, like the securing of the frequencies used for the transmission of the location data and the technical and legal guarantees, which should accompany the sub-contracting of a third party in order to ensure the confidentiality of the data.

An application decree should be published in order to define the conservation period of the data. During this period, specific police officers will be allowed access to the data with the purpose of criminal or offences inquiries, i.e. in almost all cases. The CNIL is required to give its opinion prior to the approval of the decree.

A first experiment has been launched, with the previous approval of the CNIL for 40 convicts in the context of judicial surveillance[115]. The system will process a series of data needed for

---

[113] Decision n° 2005-527 DC of 8 December 2005 on the Act on repetition's offences treatment (*sur la loi relative au traitement de la récidive des infractions pénales*).
[114] Délibération n°2006-171 du 27 juin 2006 portant avis sur un projet d'arrêté relatif à l'expérimentation du placement sous surveillance électronique mobile, JO 177 du 2 August 2006.
[115] Arrêté du 24 juillet 2006 portant création à titre expérimental d'un traitement automatisé de données à caractère personnel relatif aux personnes condamnées placées sous surveillance électronique mobile, JO 177 du 2 août 2006.

the monitoring of the convict in order to ensure he respects his obligations, and for his search and arrest in case he tries to escape.

6.3.2 Requests of location data by public authorities

Specific obligations for the retention of traffic data by Telecommunication Operators have been implemented since 2001. As a general principle, Telecommunication Operators are bound to erase or anonymise these data. Traffic data refer to any information processed for the need of the conveyance of an electronic communications by the Telecommunication Operators (Art. R. 10-12 Code of the Posts and Electronic Communications Code). It follows that location data can be part of traffic data and thus should be erased as well. However, several exceptions are foreseen, in particular for the persecution of criminal offences, when the data can be retained for up to one year. In any case, data related to the content of the communication cannot be preserved.

As a consequence, Telecommunication Operators are bound to retain traffic data in three different cases:

- Up to one year, for the needs of prosecution of criminal offences. In this case, the judicial authority could access these data upon request in the context of judicial inquiries.
- Up to one year, when their conservation is required for billing purposes.
- Up to three months, when their conservation is required for network security reasons.

The broad and vague terms used by the legislator compel the Operator to retain a large amount of data, which has been highly criticised by the CNIL. When processed for the needs of prosecution of criminal offences, Art. R 10-13 specifies the data which should be retained: the information allowing the identification of the user, the data relative to the terminal equipment and the type of communication, and the date, hour and duration of each communication, data relative to complementary services requested or used and their providers, the origin and the localisation of the communication. For telephony services, the data allowing the identification of the receiver of the communication should be retained as well.

In 2006, the Act for the fight against terrorism has established an administrative requisition procedure for the consecution of the connection and traffic data, without any previous judicial authorisation, in the context of prevention of terrorist attacks This new procedure allows police agents to request and access certain type of traffic data, for the need of prevention of terrorist attacks (article L.34-1-1 Code of Posts and Electronic Communications). In this case, a specific procedure is established in order to control the legitimacy of the request: the request should be grounded and subject to the authority of a qualified person dependant on the Ministry of Interior Affairs. The requests are recorded and communicated to the National Commission of Security interceptions' control [*Commission national de contrôle des interceptions de sécurité*]. This person is designated for a period of three years and should report once a year to this Commission. When it recognises a breach of trust or harm done to fundamental rights, it has to refer to the Ministry of Interior Affairs, which has to determine the relevant measures to be taken within 15 days.

6.4 Legal framework for processing location data by private parties

Most of the location data processing by private parties is taking place in the field of public electronic communications networks through the use of Location Based Services. These processing will thus fall under the provisions of both the Code of Posts and Electronic communications and the Data Protection Act. Specific issues rise regarding the localisation of the user of the localisation device, e.g. a mobile phone, by the subscriber of the service. Even if the service provider should rely on the previous consent of the subscriber, it is not compelled by the legislation to obtain the previous consent of the user as well. However, the processing of the user's location data by the subscriber does have to be legitimated by one of the grounds listed by Art. 7 of the Data Protection Act. The difficulties come from the fact that this article allows the processing of personal data without the previous consent of the user in some specific cases. The CNIL and the jurisprudence have the difficult task to balance these competing interests and modulated the application of the rules respectful of the fundamental rights of the data subject.

Three different cases dealt with by the CNIL will be mentioned in order to get a better comprehension of the delicate equilibrium established between freedoms and the use of Localisation Based Services in France. The first one refers to the processing of location data in the context of a labour relationship, when the employer's right to organise the work activity and the production process comes into collision with the employee's fundamental rights, such as privacy and the freedom of movement in an anonymous way. The second one refers to a case where the CNIL considered that the free consent of the data subject could not be guaranteed and thus denied the possibility of legitimating the processing on this basis. Finally, the problems raised by the control of minors by their parents through the possibility given by Mobile Operators to localise mobile phones will be presented.

6.4.1 Surveillance of employees

The processing of worker's personal data should respect not only the principles set up by data protection legislation and of Art. L.34-1 of the Code of Posts and Electronic Communications but also some specific guarantees established by Labour Law. These provisions form a complex network of obligations that the employer has to comply with:

- *Labour Law* will apply to the possibility and conditions of employees' monitoring
- The *Data Protection Act* will apply to the processing of the employees' location data by the employer
- The *Post and Electronic Communication Code* will apply to the relation between the Operator and the employer which will imply the acknowledgment of some rights to the employee who is using the device.

The use of localisation devices by the employer could be foreseen from the need of surveillance of the employees to improving work organisation through the optimisation of routes, as is the case for taxi companies. The legitimate interest of the employer and the fundamental rights of the employee will thus have to be carefully balanced.

6.4.1.1 General principles from labour law

Three general principles deriving from Labour Law apply to the processing of employee's personal data (CNIL, Cybersurveillance sur les lieux de travail, 2004:8): Proportionality, transparency and previous consultation of the representation of workers.

Proportionality

Article L120-2 of the Labour Code stipulates that: "No one can restrict personal rights and individual and collective freedoms whenever they are not justified by the nature of the task which should be accomplished, nor proportionate to the purpose." The control of the effective implementation of this principle will be dealt with by the Courts. This allows an ex-post control of the restrictions implemented by the employer to the rights and liberties of the worker, being part of the definition of the borders of private life in the workspace.

Transparency

Article L121-8 of the Labour Code introduces an obligation of information prior to the processing of the personal data of both workers and candidates collected by a device. This principle echoes back the obligation of previous information made by the Data Protection Act.

Collective Consultation

Article L432-2 of the Labour Code creates the obligation of information and consultation of the Works Council, prior to any project of introduction of new technologies when they may have consequences on the working conditions. Moreover, Article L432-2-1 stipulates that the Works Council should be consulted, before the decision of implementing in the company any technique of control of the working activity. The violation of this obligation constitutes a hindrance [*délit d'entrave*][116] (Article L438-1 of the Labour Code). The texts applying to civil service[117] established a similar obligation of information and consultation.

6.4.1.2 Data protection obligations in the Data Protection Act and the Posts and Electronic Communications Code

The CNIL has issued some general guidelines since the year 2002 regarding the cyber-surveillance of workers[118], defining the rules which should apply to this specific context. The cyber-surveillance aims at controlling the physical presence of the worker but also his precise location. Nowadays, the processing of location data allows the surveillance of the employer to go one step further and to control the movement of the employee inside or outside the workspace.

In response to the vast development of the location data processing by employers with purposes of improving the production process or of controlling the working hours, the CNIL issued a series of documents, defining the rights and obligations of controllers. First of all, a

[116] This is a punishable offence committed by a company when preventing or hindering a union from carrying out its normal duties.
[117] 7 articles 15 de la loi n°84-16 du 11 janvier 1984 et 12 du décret n°82-452 du 28 mai 1982 (fonction publique de l'Etat), article 33 de la loi n°84-53 du 26 janvier 1984 (fonction publique territoriale), article 24 de la loi n°86-33 du 9 janvier 1986 (fonction publique hospitalière).
[118] CNIL, Cyber-surveillance at workspace [*Cybersurveillance sur les lieux de travail*], March 2004, available at: <http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf>.

recommendation[119] was adopted on the implementation of devices for the localisation of vehicles used by the employee of a public or private body, based on the results of a vast consultation of public authorities, professional organisations, trade unions and location based service providers conducted during 2005. It has been followed by a simplified norm of declaration[120]. This means that the data processing which is respecting the guidelines provided by the norm of simplification is not expected to harm privacy or other fundamental rights (Article 23 of the Data Protection Act) and could benefit from a simplification of the administrative procedure for the declaration. Some general guidelines have also been issued for the controllers[121].

The CNIL recommendation only applies to the processing derived from the monitoring of professional vehicles used by the employees for the needs of their professional activity in public and private bodies. It does not apply to the *chronotypographs* of persons and goods transport drivers. Such processing is mainly based on the use of the technology GSM/GPS which permits the display on a map of the exact position of a vehicle (CNIL, 2005 Annual Report: 83). Therefore, it allows a close control of the activity of the worker. These rules could be extended to the use of other localisation devices by employees for their working activity, such as for instance, the use of mobile phones.

The main issue, which had led the CNIL to publish this recommendation, rests in the difficult balance between the right to privacy and the right of the employer to organise and control the working activity. Moreover, the use of location devices could intrude into the private life of the worker and makes more difficult the separation between professional and private life. Finally, the processing of location data could give information to the employer which goes beyond what is strictly necessary for the purpose of the processing. The data minimisation principle will act here as a specific safeguard.

Finality and legitimacy

According to the finality principle, the use of location data shall respond to a specific need linked to the employer's activity. The respect of this principle should avoid a disproportionate control upon employees (CNIL, 2005 Annual Report: 83). As mentioned above, the location data processing, in order to be legitimate, should also comply with Article L.120-2 of the Labour Code[122] and not be restrictive with regard to the rights and freedoms of individuals whenever they are not justified by the nature of the function, nor proportionate to the purpose.

On this basis, the recommendation defines a list of purposes considered as legitimate and justified:

- Improvement of security of individuals or goods carried

[119] Decision n°2006-066 of 16 March 2006 adopting a recomendation relative to the implementation of employees of a public and private bodies vehicles' localisation devices [*portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public*], J.O n° 103 du 3 mai 2006.
[120] Délibération n°2006-067 du 16 mars 2006 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés.
[121] CNIL, Droits et obligations en matière de géolocalisation des employés pa run dispositif de suivi GSM/GPS, available at: <http://www.cnil.fr/index.php?id=2056>.
[122] Article L120-2 of the Labour Code stipulates that: "No one can restrict personal rights and individual and collective freedoms whenever they are not justified by the nature of the task which should be accomplished, nor proportionate to the purpose."

- Improvement of the assignment of means to provide services in different places
- Improvement of the production process, through a better assignment of resources (e.g., the possibility of sending the closer vehicle to a specific place where the service has to be provided, such as with taxis), or indirectly for the analysis of the itineraries (e.g., analysis of time needed to achieve an activity)
- Follow-up and billing of services linked to the use of the vehicle, e.g. intervention in the road network, collection of rubbish, etc.
- The control of working hours, when it can not be achieved by other means. The processing of location data cannot be justified when the employee is free to organise its work.

Information and consent: deactivation of the device

Art. L.34.1 of the Code of Posts and Electronic Communications compel the Telecommunication Operator to obtain the previous and informed consent of the subscriber. When the subscriber is not the person who will use the device, this article recognises a right to suspend the consent given by the subscriber, i.e. deactivate the localisation device. This means that although the consent of the user is not required, he should be informed of the processing in the terms specified by this article in order to be able to suspend the consent given. In the specific case of a labour relationship, the employee is using a localisation device placed by the employer who will subscribe to the service. Therefore, only the consent of the employer is required prior to the activation of the service. However, the employer should inform the user, i.e. the employee, of the existence of the processing in the terms of Art. L.34-1.IV and of its right to deactivate the device. Here, a difficult balance should be made in order to define when the employer can compel its employees to keep the device activated and thus allows him to process the location data. This processing should be legitimated by one of the grounds listed by Art. 7 of the Data protection Act. However, as consent cannot be freely given in this situation, because of the imbalance which characterizes the labour relationship, the CNIL compel the employer to legitimate the processing on the grounds mentioned above.

Moreover, the processing of location data in the field of workspace raises two questions: the level of control an employee can be subject to, and the borders between private and professional life. The limits established by consent in the general data protection system are shaded in the workspace area, as long as the employer has his own legitimate interests to these processing.

Therefore, even if such data processing could be legitimate, they can never lead to a permanent surveillance of the employee, and thus cannot be justified out of working hours. This interpretation will be of particular importance in the case of profession which require the worker to change place of work, as for instance, medical visitors, commercial agents, etc. As a consequence, employees should have the possibility of deactivating the service out of their working hours when they are allowed to use the vehicle for private purposes. Employees with a trade union mandate should not be monitored when they act in the frame of the exercise of their mandate.

Data quality

Regarding the data collected, location data processing is providing significant quantity of information, not always relevant to the purposes. For instance, the devices put in a vehicle with the purpose of localisation could provide information relative to the kilometres made, the

speed average, the maximum and minimum speed, and even the way of driving. The processing of these data could lead into the recognition of offences and thus cannot be carried out by private bodies. Article 9 of the French Data Protection Act stipulates that the processing of personal data relating to offences, convictions and security measures may take place only by: the courts, public authorities and legal entities that manage public services, within the framework of their legal remit; the representatives of the law for the strict needs of the exercise of the functions granted to them by the law; the legal persons mentioned in Articles L321-1 and L331-1 of the Intellectual Property Code, acting by virtue of the rights that they administer or on behalf of victims of infringements of the rights provided for in Books I, II and III of the same Code, and for the purposes of ensuring the defence of these rights.

Confidentiality

The persons who can access the data should be limited to the sole persons who need it for the accomplishment of their activity (e.g., persons in charge of the planning or coordination process, persons in charge of security of the transport and shipment of persons and goods, or the human resources head). Besides, relevant security measures required to guarantee the confidentiality of the data should be implemented. At least, the individual access to the data should be protected by a UserID and a password, regularly renewed, or by any other means of identification.

Retention of the data

Regarding the storage period of the data, the CNIL considers that a period of two months is not excessive. However, the data can be preserved for longer periods for historic purposes or for optimising the organisation, or to prove the services provided, whenever it is not possible to prove it by other means. Moreover, the data can be preserved up to one year in case the service is being challenged. In other cases, the controller shall refer to the existing legal provision, e.g. in case of the control of working hours through location based systems. Only the data related to the working hours should be stored for a period of up to five years, while the location data should be erased.

6.4.2 Processing of location data by Insurance Companies

The following case illustrates another situation where consent is not considered as sufficient grounds for the processing of location data, in the context of localisation of third parties, i.e. where the subscriber and the user are two different persons.

An Insurance Company submitted to the CNIL a project of a new insurance policy aimed at young drivers and based on the processing of the speed of the vehicle and hours of driving. In the new policy, the driver agrees not to drive during the nights of Saturdays, Sundays and bank holidays between 2 a.m. and 6 a.m. and to be monitored in order to ensure he respects his contractual obligations, in exchange for a reduction in price. He agrees that the Insurance Company processes his data relative to location, speed, type of road, hours and driving duration. The data would be sent through a device placed into the car every two minutes. The insurance policy would include an assistance service in case of accident, breakdown and theft.

This processing has not been authorised by the CNIL,[123] on the ground that monitoring all the driver's movements does not comply with the legal requirement of proportionality, as long as it is exclusively implemented for the ensuring the respect of the contractual obligations of the driver. Besides, the CNIL considers that the systematic collection of vehicle location data with the purpose of modulating insurance rates harms the freedom of movement in an anonymous way in an unjustified manner.

Moreover, in this specific case, this processing could fall under the prohibition of Article 9 of Data Protection Act as it could lead to recording data related to offences. As mentioned above, such processing should be authorised by the CNIL (Article 25-3 Data protection Act) and cannot take place by Insurance Companies.

This example illustrates the fact that consent does not constitute by itself a legitimate ground to justify all processing of location data. The processing of these personal data has important implications for the right to have a private life but also for the freedom of movement in an anonymous way.

6.4.3 Processing of minors' location data

Another problematic case raised by Location Based Services is the localisation of minors by their parents. Once again, the legitimacy of the processing and the grounds the parents should use to be able to access to the location data of their children is raising a number of important issues. In this case, the Mobile Operator provides to the subscriber, i.e. the parents, each time he requests it, the location of the mobile phone, i.e. of the minor. This service raises the problem of the application of data protection rules to minors, and in particular whether minors should give their consent to the processing or the parental authority is sufficient to legitimise the processing.

In France, no specific legislation regarding the localisation of children has been enacted. Therefore, the rules set up by Art. L.34-1 of the Code of Post and Electronic Communications applies to this kind of processing. The minors, who in this case are the user, have a right to object to the processing as users of the services, and should be informed before the processing takes place. The CNIL required that the service providers obtain the previous consent of the child, who has to authorise the first subscription through SMS, and they inform the child of each request of localisation. Moreover, it usually requires the Service Providers to inform users about the risks of an abusive use of the service (D. Gasse, Proteccion de datos personales y geolocalizacion, 2006).

In 2002, after the approval of Directive 2002/58/EC, the CNIL had launched a public consultation, in order to get feedback from citizens, as the problem is broader than a strict application of data protection rules and implies considerations related to education. The working assumption was that this system should be discussed as long as it might not be the most adequate for educating minors. The principle of parental authority could not always justify the collection of the consent of the child.

The results of the public consultation shows that 85% of the parents think this service is more or less legitimate, on the basis of an improvement of the security of the child. Only 20% of the parents are opposed to this processing, while 57% thinks it is completely legitimate. Some

[123] CNIL, Délibération 2005-278 du 17 novembre 2005, portant refus de la mise en oeuvre par la MAAF Assurances SA d'un traitement automatisé de données à caractère personnel basé sur la géolocalisation des véhicules.

of the parents highlight the risk of "responsibility depreciation" (*deresponsabilisation*) of the parents, while many think that this processing can be justified by their general obligation of control derived from the parental authority, or consider it is a just compensation for the payment of the communication of the child.

According to the survey, the control would mainly affect minors between 13 and 16 years (high school). Above 16 years, the children gain more autonomy from their parents who do not feel the need to localise them anymore. The question of autonomy and trust in the parent-children relationship is the main argument of parents opposed to this processing.

Regarding the consent of the minor, 45% consider that it constitutes an appropriate guarantee, 38% think that the child is not really free, and 18% does not even think they should need to ask their child for their agreement.

No action from the CNIL has been taken so far, nor is any expected.

6.5 Conclusion

The actual legal framework applying to location based processing is based on two different norms, the Code of the Posts and Electronic Communications and the Data Protection Act. Specific issues have been raised in the field of Location Based Services when they allow the subscriber to localise the device used by a third party. The Courts and the CNIL should make the balance between the different interests at stake, on a case-by-case basis, but few decisions have been made so far regarding this topic, which makes it difficult to draw conclusions on future trends or positions of both authorities.

Both the CNIL and the Court have measured the risk of the processing of location data which do not only affect the right to have a private life but rather the freedom of movement in an anonymous way. In some cases, other factors interfere, such as education issues in the case of the processing of minors' data. Therefore, such processing appears to be highly sensitive and is considered as legitimate only when the purpose cannot be achieved by any other means less intrusive. As a consequence, consent is a necessary but not a sufficient condition to the processing.

Regarding the processing for national security purposes, the Data Protection Act poses some limits through the issuing of the opinion of the CNIL which, despite not being binding, remains influential. However, the State remains free not to follow the opinion of the CNIL which is not binding. When the processing is foreseen by a law, the Constitutional Council can operate a control of validity but it remains abstract. Moreover, this institution is willing to validate processing of personal data whenever they consider their justification is in the security of individuals. For instance, the approval of the Act for the fight against terrorism has shown that the Opinion of the CNIL was not always followed and some provisions of the law relative to the systems of surveillance considered harmful by the CNIL have not been modified, such as the automatic taking of photographs of vehicle passengers at certain roads. The Constitutional Council has validated these same provisions.

7 Location Information from a German Perspective

Maren Raguse (ICPP)

7.1 Introduction

Only a few years ago services which take into account the location of the user were expected[124] to find wide use within a short timeframe as technologies for determining the geographic location of cell phones and other mobile devices have become increasingly available. A survey carried out in 2003 by the registered association of German Internet enterprises (eco) came to the result that the success of Location Based Services (LBS) would determine the future of mobile business.[125] 76% of the interviewed experts considered LBS a key factor for the success of mobile business and forecasted a breakthrough of Location Based Services in 2005. However, the German market for Location Based Services has not expanded as predicted by providers of such services.[126] By now all German mobile network operators offer Location Based Services. Still, a breakthrough of LBS in mobile networks is expected as the use of sophisticated mobile devices such as smart phones, fast UMTS data transmission in combination with more exact location technologies using satellite positioning technology like GPS, A-GPS or from 2008 Europe's Galileo has increased. Slow WAP transmission, poor accuracy of location data resulting from GSM positioning using cell-ID and rather poor graphic displays of mobile devices allowing only the presentation of LBS results as text, belong to the past.

The variety of Location Based Services is broad. Services available in Germany include navigation, community-services like buddy tracking[127], services enabling the positioning of a cell-phone in case of an emergency[128] or upon a differently motivated request[129], automatic payment services or fleet management[130]. Also, electronic bracelets for elderly disoriented persons are offered allowing carers to position the cared-for person using GSM accuracy.[131] Furthermore, a GPS tracking service for children is also available.[132]

Location information of data subjects using mobile devices is very sensitive with regards to privacy as it may enable the tracking of data subjects. Location data can also enable social and

---

[124] ECIN, Location Based Services – Standortvorteile nutzen, 29th of March 2001. Available at: <http://www.ecin.de/mobilebusinesscenter/lbs/index.html>.
[125] Verband der deutschen Internetwirtschaft e.V. (eco), eco-Studie: Location-Services erfolgskritisch für M-Business, 23rd of April 2003. Available at: <http://www.eco.de/servlet/PB/menu/1204471_l1/index.html>.
[126] Silicon.de, LBS: Mauerblümchen mit dem Zeug zum Superstar, 4th of May 2006. Available at: <http://www.silicon.de/enid/umts/14266>.
[127] The service "Buddy Alert" is offered by MOBILOCO GmbH: <http://www.mobiloco.de/subpages/buddy/0100.php>.
[128] The service "Notfon D" is offered by the car insurance association's emergency call service: <http://www.gdv-dl.de/notruf/ortung.html>.
[129] GSM positioning is offered by Corscience GmbH & Co. KG: <http://www.corscience.de/ortungssystem.html>.
[130] Positioning of vehicles is for example offered by virtic GmbH: <http://www.virtic.net/?u=home> or tomtom work: <http://www.tomtomwork.com/de/products/product.xml>.
[131] The system is called "Senior Track": <http://www.corscience.de/shop/product_info.php?info=p8_Senior-Track.html>.
[132] Services available are called "LiveService Kids": <http://www.steiger-stiftung.de/lifeservice/lifeservice_kids_was.php> and "track your kid", <http://www.track-your-kid.de/>.

behavioural profiling.[133] It is possible to distinguish between proactive and reactive Location Based Services. For proactive LBS the user is continuously tracked in order to recognise events relevant for the LBS. This could for example be a target reaching a point of interest or a specific threshold value[134]. For a reactive location based service the user of the mobile device requests a service based on his location and on actual demand. In this case the user initiates a limited tracking of his current position at the moment he requests a service[135]. With regards to transparency and obtaining the data subject's distinct consent for a positioning process, reactive LBS require a conscious action triggering or approving localisation and therefore reduces the possibility of unobserved tracking of a person.

The Federal Data Protection Commissioner (BfDI) has on several occasions[136] addressed privacy concerns with regards to LBS. Tracking services allow secret surveillance without the data subject's knowledge and security mechanisms like a confirmation SMS requesting the tracking can be circumvented without the data subject being aware simply by using the cell phone for a couple of unnoticed minutes. The Commissioner stated that he was currently debating with the Federal Ministry of Justice to introduce a provision which would turn secret positioning of individuals into a criminal offence.[137] Furthermore, he voiced concerns with regards to recent developments in the insurance sector. Insurance companies have tested "pay as you drive" car insurance. Cars are equipped with an "on board unit" (OBU) which uses GPS to collect detailed information on actual driving behaviour (roads used, time of driving, travelled kilometres) and GPRS to transmit this information to a service provider. The service provider automatically analyses this information to assess the level of risk associated with the specific route taken at the specific time, also taking into account who drove the car (e.g. the owners child who just got his licence or a skilled driver who in 30 years has not had even one accident). Commissioner Schaar, who currently heads the Art. 29 data protection working party, said he would bring this issue to the attention of the working party as the technology bears risks to the privacy not only of the car owner but also of other people who drive the car. Pay as you drive enables a constant surveillance and the BfDI stressed his apprehension that the comprehensive driving data could be linked with other data for further profiling or be accessed by law enforcement authorities. Schaar warns uncontrollable databases may be established.[138]

Private parties wanting to access location data of third parties (like employees) which was collected by telecommunications service or location based service providers will not find

---

[133] See: Fritsch L. 2005: 'Mind your Step! How Profiling Location reveals your Identity – and how you prepare for it', 2005.
[134] See: Treu G., Küpper A. & Ruppel P.2005: 'Anonymization in Proactive Location Based Community Services', 2005.
[135] See: Küppers A. & Treu G. 2005: 'From Location to Position Management: User Tracking for Location-based Services', 2005.
[136] See:
<http://www.bfdi.bund.de/cln_029/nn_531474/sid_669D26107CF2FB61D80EBD256563E01B/DE/Themen/KommunikationsdiensteMedien/Telekommunikation/Artikel/LocationBasedServices.html__nnn=true,
http://www.bfdi.bund.de/cln_029/nn_533554/SharedDocs/Publikationen/PM12-04LocationBasedServices__LBS__NurMitEinwilligungDerNutzerZulaessig,templateId=raw,property=publicationFile.pdf/PM12-04LocationBasedServices_LBS_NurMitEinwilligungDerNutzerZulaessig.pdf>.
[137] Commissioner Peter Schaar in an interview with NDR Info, 2 February 2007. See:
<http://www.pressrelations.de/new/standard/dereferrer.cfm?r=266193>.
[138] Gläserne Autofahrer für Versicherungen und Fahrzeughalter, 13 April 2006.
<http://www.bfdi.bund.de/cln_030/nn_531474/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2006/VDIInterviewGlaesernerAutofahrer.html__nnn=true>.

specific regulations in place covering this case. The general provisions of the Federal Data Protection Act[139] (*Bundesdatenschutzgesetz, BDSG*) and the Telecommunications Act are thus applicable.

This section will look into the access to location data by public parties (law enforcement authorities) and private parties (employers). A definition of location data is laid down in the Telecommunications Act[140], which transposed Directive 2002/58/EC. The provisions transposing Directive 2002/58/EC will be described in detail. These regulations are not the only provisions referring to the location of an individual in German law. An overview of additional laws will be given. Furthermore, the provisions applicable to the provision of Location Based Services will be presented.

7.2 Legal framework: general principles

7.2.1 Collection, processing and use of personal data

German data protection law is regulated in the Federal Data Protection Act, the Data Protection Acts of the German states and regulations in specific fields of law.

Scope of the federal Data Protection Act

The Data Protection Acts of the German states are applicable if the controller is a public body of the respective state. The Federal Data Protection Act is applicable if the controller is a public body of the Federation[141] or a private body[142].

The Federal Data Protection Act was passed in 1977. Germany did not transpose Directive 1995/46/EC within the set period of three years. On 23 May 2001 the Federal Data Protection Act was modified to implement the directive into German law. Of the sixteen German states only Hesse and Brandenburg kept the date for transposing the Data Protection Directive into national state law. This report will focus on the regulations laid down in the Federal Data Protection Act, as Location Based Services are provided by private bodies and the legal requirements for the provision of LBS are to be found in the Federal Data Protection Act, the Telecommunications Act and the Telemedia Act[143].

As a general rule, the collection and processing of data identifying an individual or relating to an identifiable person in Germany requires a statutory basis or the consent of the data subject. Without these the collection and processing is illegal. A definition of personal data is laid down in Article 3 paragraph 1 BDSG: “Personal data means any information concerning the

---

[139] Bundesdatenschutzgesetz (BDSG). An English translation is available at: <http://www.bfdi.bund.de/cln_030/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf>.

[140] Telekommunikationsgesetz (TKG). The Federal Ministry of Economics and Technology released an English translation of the Telecommunications Act which can be accessed here: <http://www.bmwi.de/BMWi/Redaktion/PDF/Gesetz/telekommunkationsgesetz-en,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf>.

[141] These are the authorities, the bodies of the judicature and other public-law institutions of the Federation, of the Federal corporations, establishments and foundations under public law as well as of their associations irrespective of their legal structure, Art. 2 paragraph 1 BDSG.

[142] Private bodies means natural or legal persons, companies and other private-law associations, Art. 2 paragraph 4 BDSG.

[143] Telemediengesetz (TMG). The TMG is effective from 1 March 2007.

personal or material circumstances of an identified or identifiable individual (the data subject)". If data allows determining the location of a natural person at a specific point in time, this information is personal data. The collection, processing and use of location data must comply with the provisions laid down in the Federal Data Protection Act, if no specific regulation for a specific kind of location data is applicable.

Generally, the Federal Data Protection Act is ruled out if a specific law is in place regulating a field of law. The following figure presents the general relation of provisions covering the use of personal data in German law.

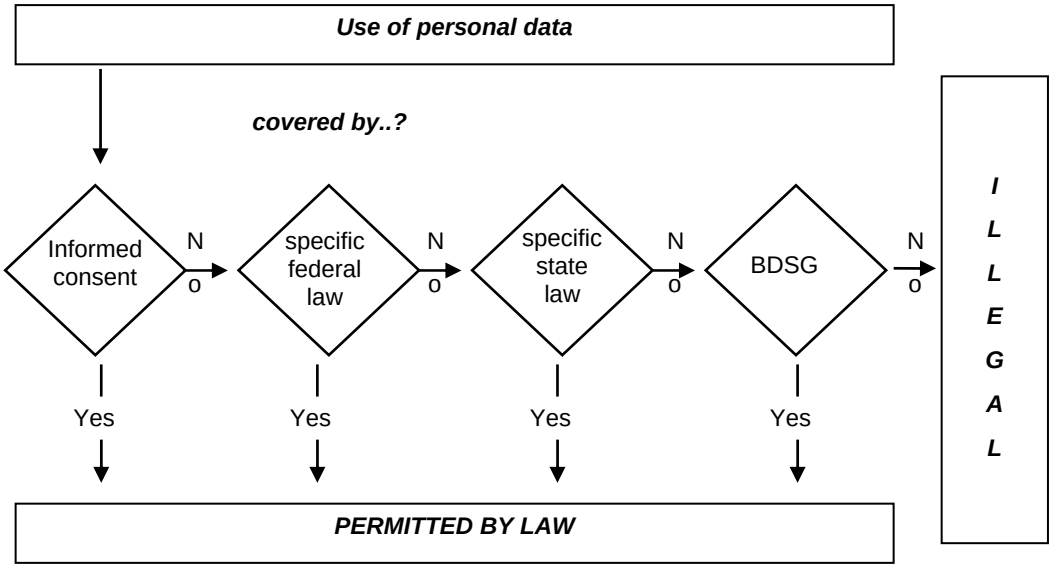

Figure 6: Order of application of legal bases[144]

The Federal Data Protection Act provides general rules on the collection, processing and use of personal data.

General privacy principles

General privacy principles as laid down in the OECD Guidelines, Convention 108 and the Data Protection Directive have been transposed into German law and are regulated in the federal and state data protection acts. These principles include the purpose binding principle, the proportionality principle, transparency of processing and furthermore obligations with regards to the quality and security of data.

According to Article 27 and 28 BDSG private parties may collect and process data only compliant to a previously defined purpose. This purpose must be legitimate, that means it must be covered by existing legal requirements or the data subject's consent, Article 4 paragraph 1 BDSG. The data collected and processed must be necessary to achieve the previously defined purpose and the intrusion to the right to personal self-determination shall not be excessive in relation to the pursued purpose. The data subject shall be aware of his data being processed. In order to achieve this transparency, several measures are installed. As a

[144] Modified from Tinnefeld M.-T. et al. 2005. Einführung in das Datenschutzrecht, 2005, page 317.

general rule, data must be collected from the data subject to cause awareness, Art. 4 paragraph 2 BDSG. Upon collection information must be provided by the controller as to the identity of the controller, the purposes of collection, processing and use and the categories of recipients, Art. 4 paragraph 3 BDSG. The data subject's consent (Art. 4a BDSG) to data collection, processing and use shall be effective only when it is based on the data subject's free decision. The consent must be an informed consent. This means the data subject shall be informed of the purpose of collection, processing or use and of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. Finally, the data subject shall be notified if his personal data is stored for the first time without his knowledge, Art. 33 BDSG. Several rights of the data subject shall ensure the quality of data. The data subject may request information on stored data concerning him, including any reference in them to their origin and recipient, the purpose of storage and recipients or categories of recipients, Art. 34 BDSG. This right to obtain information is required to then be able to exercise the right to correction of incorrect data, erasure of data if their storage is inadmissible, or the blocking of data, Art. 35 BDSG. Finally, controllers must ensure the security of data by technical and organisational measures as set out in the annex to Article 9 BDSG.

After giving an overview of the provisions of the transposition of Directive 2002/58/EC by means of modifying the Telecommunications Act, a description of the legal requirements for Location Based Services will follow.

7.2.2 Transposition of Directive 2002/58/EC

The most distinct definition of location data is laid down in the Telecommunications Act. Directive 2002/58/EC on privacy and communications[145] was transposed into national law by means of a modification of the Telecommunications Act passed on 26 June 2004. Germany did not keep the fixed period for transposition laid down in Article 17 of the Directive which required a transposition before 31 October 2003. The changes in the Telecommunications Act were subject to extensive parliamentary debate in the mediation committee of the Upper and the Lower House of Parliament. In Articles 91 to 107 the modified Telecommunications Act now contains a new part regulating data protection in the communications sector.

The provisions of the Telecommunications Act (TKG) apply if personal data of telecommunications subscribers and users is collected or used by companies or persons providing telecommunication services on a commercial basis. The Telecommunications Act applies in place of the Federal Data Protection Act, being the specific regulation with regards to the processing of personal data in the electronic communications sector. The Federal Data Protection Act supplements the Telecommunications Act if the latter does not conclusively cover a case. The right to obtain information as well as the right to correction of incorrect data, erasure of data if their storage is inadmissible, or the blocking of data is based on the BDSG also in the context of processing of data of telecommunications subscribers.

7.2.2.1 Customer data, traffic data or location data

The provisions of the TKG differentiate between three types of personal data usually collected and used for the provision of telecommunications services. Customer data is defined as the data of a subscriber collected for the purpose of establishing, framing the contents of,

[145] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

modifying or terminating a contract for telecommunications services, Art. 3 lit. 3 TKG. Traffic data means data collected, processed or used in the provision of a telecommunications service, Art. 3 lit. 30 TKG. And location data means any data collected or used in a telecommunications network, indicating the geographic position of the terminal equipment of an end-user of a publicly available telecommunications service, Art. 3 lit. 19 TKG. Furthermore, the Telecommunications Act provides a definition of a location based service: 'Value added service means a service which requires the collection and use of traffic data or location data beyond that which is necessary for the transmission or billing of a communication', Art. 3 lit. 5 TKG.

The collection and use of customer data is regulated in Art. 95 TKG.

Customer data comprises

- name and address of subscriber,
- banking information and
- the kind of contracted service.

The focus of this report is on an analysis of the collection and use of location data. By means of the customer data collected the geographic location of terminal equipment can be linked to a natural person.

The collection and use of traffic data is regulated in Art. 96 TKG. This provision transposes Art. 2 lit b) of the Directive on privacy and electronic communications.

Traffic data comprises

- the calling telephone number,
- the numbers dialled or other identification of the lines in question,
- the location data, if mobile handsets are used,
- the beginning and end of a connection,
- the telecommunications service used by the user,
- the termination points of fixed connections, the beginning and end of their use,
- any other traffic data required for set up and maintenance of the telecommunications service and for billing purposes.

The retention period for traffic data is regulated in Art. 96 paragraph 2 TKG. According to this provision traffic data may be used after the termination of a connection only where required to set up a further connection or for the purpose of

- charging and billing,
- itemised billing,
- detection, location and elimination of faults and malfunctions in telecommunications systems,
- information on incoming calls.

If none of the listed exemptions apply, traffic data currently are to be erased by the service provider without undue delay following termination of the connection. Transposing Directive

2006/24/EC on data retention will substantially extend this retention period. Germany has chosen to introduce the shortest retention period possible and will require a six-month retention of traffic data. The Federal Ministry of Justice issued an unofficial draft for a transposition law[146].

The collection and use of location data is regulated in Art. 98TKG. This provision was introduced in the cause of harmonisation of TKG with Directive 2002/58/EC. Prior to 2004 no regulation on location data and value added services existed in German law and the legal subsumption bared difficulties. Location data relating to users of telecommunications services may be processed only when they have been made anonymous or with the consent of the subscriber to the extent and duration necessary for the provision of value added services. The subscriber is obliged to inform his co-users of all such given consent. Consent may be withdrawn at any time. Currently, location data may only be stored to the duration necessary for the provision of the LBS.

The Cell-ID is considered a location date, which at the same time is necessary for the conveyance of the service and is thus also regarded a traffic date. Location data not required to establish a connection with the mobile handset but collected for other purposes is considered location data, too. It is possible to differentiate between location related traffic data and precise location data.[147]

7.2.2.2 Requirements for information provision and consent by electronic means

When concluding a contract, service providers shall inform their subscribers of the nature, extent, place and purpose of the collection and use of their personal data in such a way that the subscribes are given notice, in a readily comprehensible form, of the basic data processing facts, Art. 93 TKG. This duty to provide information includes information on which kind of location data is processed, the purpose of processing and the retention period.[148] If, for the provision of a location based service it is necessary to transmit personal data to third parties, this information shall be provided, too.

The service-provider may use subscriber-related traffic data used by the provider of a publicly available telecommunications service for the provision of value added services for the duration necessary only where the data subject has given his consent to such use, Art. 98 TKG. While Art. 4a BDSG as a general rule requires a written consent of the data subject, the Telecommunications Act lays down a specific provision for consent by electronic means in Art. 94 TKG. According to this provision consent may also be given electronically where the service provider ensures that:

- the subscriber or user has given his consent deliberately and unequivocally,
- consent is recorded,

---

[146] Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG. Available in German at: <http://www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/de-recht/RefETeil1neu.pdf>.
[147] Jandt S. 2007. Datenschutz bei Location Based Services – Vorraussetzungen und Grenzen der rechtmäßigen Verwendung von Positionsdaten, 2007, page 74.
[148] Ohlenburg A. 2004. Der neue Telekommunikationsdatenschutz – Eine Darstellung von Teil 7 Abschnitt 2 TKG, 2004, page 432.

- the subscriber or user can access his declaration of consent at any time, and
- the subscriber or user can withdraw his consent at any time with effect for the future.

The Telecommunications Act differentiates between a subscriber of a telecommunications service and user of telecommunications services. According to Art. 3 lit. 20 TKG subscriber means a natural person or a legal entity who or which is party to a contract with a provider of telecommunications services for the supply of such services. User means a natural person using a telecommunications service for private or business purposes, without necessarily having subscribed to that service. The child or husband using the mother's or wife's cell-phone is therefore a user with regards to TKG provisions.

Consent to use of location data not anonymised can be given only by the subscriber, Art. 98 paragraph 1 TKG. The subscriber shall inform his co-users of all such given consent. This regulation contradicts Art. 6 paragraph 3 and Art. 9 paragraph 1 of Directive 2002/58/EC that require consent of subscriber and user. Reasons given for this derogation of Directive 2002/58/EC are telecommunications service providers' lack of awareness of users other than the subscriber and impossibility to link location data to other individuals than the subscriber whose customer data was collected upon subscription.

7.2.2.3 Billing

While Art. 96 TKG regulates which data may be collected as traffic data at all, Art. 97 TKG lays down the requirements for their further use for billing purposes. Service providers may use traffic data only to the extent that the data are required to charge and bill their subscribers. Currently, traffic data not necessary for billing must be erased following termination of the communication.

7.2.3 Legal Requirements for Location Based Services

Location information of data subjects using mobile devices is very sensitive with regards to privacy as they allow positioning of the cell phone user at any given time. The service provider is enabled to address its customer personalised and with regards to his local surrounding. Location data can be aligned and utilised for creation of extensive and meaningful customer profiles, allowing conclusions with regards to relations and habits of the data subject as well as prediction of future behaviour.

At least three parties are involved in the provision of a network based LBS using GSM localisation:

- the content provider who offers the content of the LBS,
- the telecommunications service provider,
- the user.

As described before, the legal requirements for the personal data of telecommunications service subscribers and users are laid down in the Telecommunications Act and the Federal Data Protection Act. For the provision of a LBS a third Act must be considered in addition. Since March 2007 the content of a 'telemedia service' must comply with the Telemedia

Act[149]. Telemedia services are all electronic information or communication services which are not telecommunications services[150]. The content of a LBS is regarded a telemedia service as it exceeds common telecommunications services like voice communication, sms and provides new, multimedia content. The following figure exemplifies the relation between the parties involved in the provision of LBS.

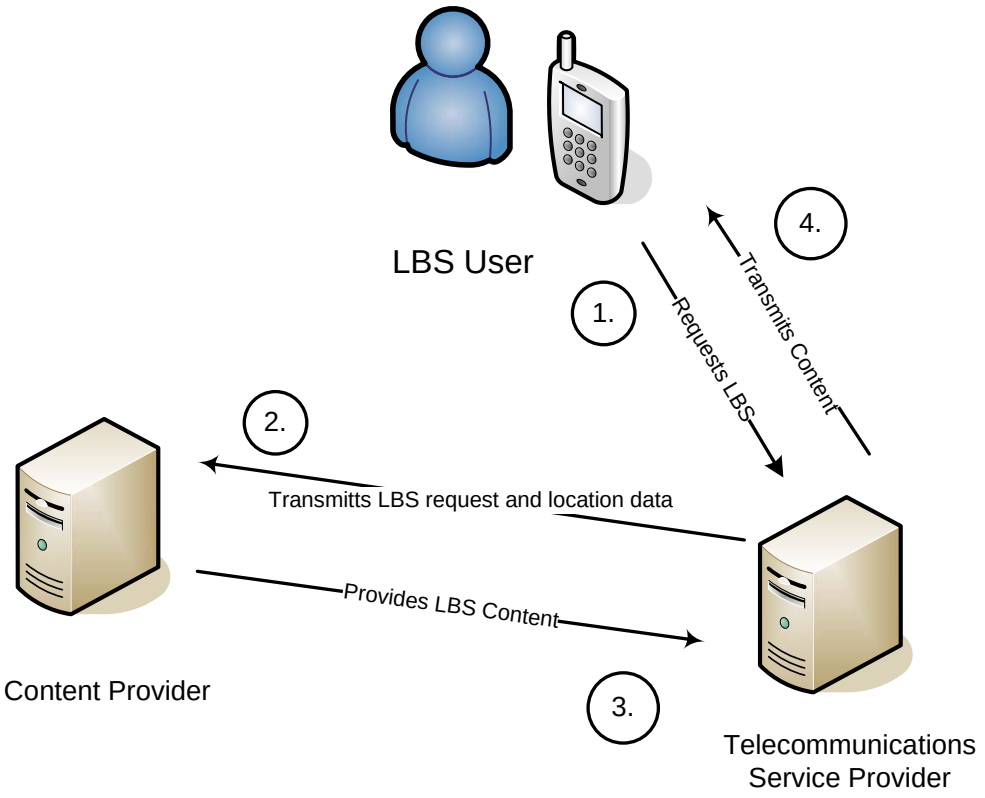

Figure 7: Parties involved in network-based reactive LBS provision

While a three-sided relation is common, the telecommunications service provider can also be providing the content of the LBS. The relation is then two-sided. The above figure illustrates that a content provider can only create a profile for one section of all services requested by the user. It is the telecommunications service provider who could link information on all services used and all location data processed.

	Covered by TMG	Covered by TKG
Collection of location data by TSP to convey telecommunications service		+
Transmission of location data from TSP to CP		+

[149] Telemediengesetz (TMG). The draft law is available in German at: <http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/elgvg-elektronischer-gesch_C3_A4ftsverkehr-vereinheitlichungsgesetz,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf>.

[150] A definition of telecommunications services is given in Art. 3 lit. 24 TKG: 'Telecommunications services means services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks used for broadcasting'.

Use of location data to provide content	+	

Table 8: Overview of use of location data and applicable law

The content provider has to comply with the provisions set out in the TMG and the telecommunications provider must comply with the regulations of the TKG. TKG and TMG cover different obligations and rights for the user, content provider and telecommunications service provider. It is therefore necessary to examine compliance separately for the content provider and the telecommunications provider.[151] The transmission of location data from the telecommunications service provider (TSP) to the content provider (CP) usually is within the scope of the Telecommunications Act, while the use of location data to provide the LBS is covered by TMG.

7.2.3.1 Collection of location data for conveyance of communication

The collection of location data initially is conducted by the telecommunications service provider to convey communication and in this context is location related traffic data. Art. 96 paragraph 1 lit.1 and 5 TKG allows collection of location data (in this case the Cell-ID) as it is necessary for set up or maintenance of the telecommunications connection. At this point, there is no relation of the location data to the latter use for LBS provision. The later use for LBS provision follows a new purpose.

7.2.3.2 Transmission of location data

The legitimacy principle applies if personal data collected for a specific purpose is to be used for a new purpose. The use for a new purpose is permissible only if a statutory basis allows the specific further use. The further use of location data for LBS provision is not permitted by Art. 96 paragraph 1 TKG as this provision requires erasing by the service provider without undue delay following termination of the connection. Location data is not covered by the exemptions in paragraph 2 which allow longer retention. The obligation to delete location related traffic data immediately after termination of the connection does not apply if further retention or use can be based on a different legal basis. In this context Art. 98 TKG allows the use of location data that is not anonymised if the data subject consented to this use. This consent may not only cover location related traffic data but also precise location data.

7.2.3.3 Use of location data for provision of LBS

The content provider may use location data for the provision of a LBS only if use is covered by a statutory basis or the data subject has consented. Articles 11 to 15 TMG lay down regulations for the use of personal data in the context of telemedia service provision.

The Telemedia Act differentiates between customer data (Art. 14 TMG), data concerning the service provision (Art. 15 TMG) and billing data (Art. 15 paragraph 4 TMG). Customer data comprises

- name,
- address,
- customer reference number,
- profile data (hobbies, taste, preferences).

[151] Jandt S. 2007. Datenschutz bei Location Based Services – Vorraussetzungen und Grenzen der rechtmäßigen Verwendung von Positionsdaten, 2007, page 74.

Data concerning service provision comprises

- profile data when used for provision of specific service,
- location data.

Billing data comprises

- bank details.

The content provider shall use personal data only if necessary to enable use of the telemedia service, Art. 15 TMG. Provision of LBS must be covered by the purpose of the contract. LBS provision is possible only if data on the location of the data subject is processed. The data subject's consent to the further use of location data for LBS provision is thus not required by the TMG. The LBS request can only be met if location data is processed. The TMG (Art. 13 TMG) however obliges the content provider to inform the data subject at the beginning of the LBS use as to

- kind of data collected and used,
- scope of data collected and used,
- purpose of data collection and use.

As consent is obligatory at the stage of collection of location data by the telecommunications provider, the lack of a second obligation to obtain consent for the content provider does not lever out the right to informational self-determination.

On a European level a distinction between telecommunication services and telemedia services does not exist. The German legal requirements for the collection and use of location data for the provision of LBS does meet the requirements set out in Art. 9 paragraph 1 of the Directive on privacy and electronic communications as it requires consent at the early stage of data collection.

7.3 Legal framework for processing location data by public authorities

Law enforcement authorities have two means of accessing data on the whereabouts of a suspect. One can differentiate between access to data collected with own technical means in the cause of an investigation (generating data) and access to data collected and processed by private parties, mostly providers of telecommunications services and Location Based Services (using data). An investigation method resulting in the collection of location data is police observation by means of special technical aids. In addition, law enforcement authorities can access traffic and location data collected by telecommunications service providers. Collection of and access to location data by law enforcement authorities is regulated in the German Code of Criminal Procedure (*Strafprozessordnung – StPO*). Transparency for and prior consent of the data subject to be located is restricted by covert investigation methods and would generally jeopardize the success of a covert investigation. In such a case notification of the data subject is required after the investigation.

7.3.1 Law enforcement authorities' access to or collection of location data

A number of German laws contain provisions concerning the location of citizens. For law enforcement authorities these include Articles 100f, 100g and 100i of the German Code of Criminal Procedure[152]. Article 100i StPO allows the positioning of a person by means of locating the position of that person's cell phone in order to prepare arrest by law enforcement authorities. Article 100f StPO allows the planned monitoring (observation) of suspects to criminal offences of considerable importance. An observation may be carried out employing special technical aids such as night-vision equipment, tracking systems and satellite-guided positioning systems or an IMSI-Catcher. Furthermore, according to Article 100g StPO providers of telecommunications services can be ordered to hand over traffic data necessary for the investigation of a criminal offence of considerable importance or a criminal offence committed by means of a 'communication terminal' (*Endeinrichtung*). Traffic data to be handed over includes the Cell-ID (*Standortkennung*) when mobile handsets are used or the termination points of fixed connections. These investigation methods require a warrant.

7.3.2 The Data Retention Directive and location data

Currently location data may only be processed for the duration necessary for the provision of a value-added service. A telecommunications service provider may store traffic data only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

The German transposition of the Data Retention Directive will extend the retention period to six months also for location data. In order to identify the location of the mobile equipment at the time of the communication the draft transposition law requires the retention of the location label (Cell-ID) at the beginning of a communication, both of the calling and the dialled number, Art. 110a paragraph 2 TKG-E.

This requirement will apply to location related traffic data (Cell-ID). The provisions of Directive 2006/24/EC do not cover precise location data and also the German draft transposition law does not extend the scope of data retention to precise location data. The Data Retention Directive still allows for up to six months the retroactive reconstruction of movements.

7.3.3 Radio cell query

In this context a method of investigation for German police gains a new scope and the proportionality of the directive has been questioned. Based on a warrant law enforcement authorities can obtain traffic data of all GSM subscribers who at the time a serious crime was committed were in range of the radio cell closest to the crime scene. This method of obtaining past traffic data of all individuals using a telecommunications service close to a crime scene is called radio cell query (Funkzellenabfrage) and is based on Art. 100g StPO[153]. What data law enforcement authorities obtain has not been precisely revealed to data protection supervisory authorities. The data used for identifying these persons must contain the Cell-ID to establish the spatial linkability. Furthermore, to identify the subscriber linkability can be established by

---

[152] Strafprozessordnung (StPO). Available at: <http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf>.
[153] Section 100g of the German Code of Criminal Procedure: 'If certain facts substantiate the suspicion that a person was the perpetrator or inciter, or accessory, of a criminal offence of considerable importance […] it may be ordered that those who provide telecommunication services on a commercial basis without undue delay disclose telecommunications traffic data as far as necessary for the solving of the crime.'

means of the MSISDN (Mobile Subscriber Integrated Services Digital Network Number), which refers to a particular mobile device. The customer data collected upon subscription allows linking the MSISDN to an identified person.

The radio cell query investigation method has been criticised as it involves innocent individuals who find themselves questioned in investigations into crimes of considerable importance. In this context the observation is crucial that once police has collected personal data the likeliness of quick deletion of data varies.[154] Being at the wrong place at the wrong time may lead to an entry 'questioned in the cause of a murder investigation'.

7.3.4 Automatic car number plate scanning

In several German states the police laws have been amended and do now contain provisions on automatic car number plate scanning. Most recently, in February 2007, the legislative assembly of the state of Schleswig-Holstein amended the state's police law[155]. Article 184 paragraph 5 LVwG-SH now allows automatic car number plate scanning. CCTV systems collect the number plate data and match it to a reference database of stolen cars or cars sought for another reason, for example because an arrest warrant was issued against the owner of the car. The data collected includes the number plate information, place of data collection, point of time of collection, and direction of travel. If the matching process does not result in a hit, the data must be deleted immediately. The automatic number plate scanning aims at identification and localisation of either a wanted car, a wanted owner of a car, or a wanted driver of a car. This investigation method, like the positioning of a suspect's cell phone, is based on the assumption that the registered car owner or driver is mainly driving the car.

7.3.5 Electronic monitoring of convicts released on parole

The state of Hesse started testing the use of electronic bracelets for convicts in 2000 and is currently the only German state using electronic monitoring of convicts released on parole. The test merged into regular use without a complete technical evaluation.[156] Several states have been discussing the use of electronic monitoring. The electronic monitoring in Hesse is based on Article 56 lit. c Criminal Code[157] and in addition the consent of the convict to be monitored. The convict, when released on parole can be instructed to not visit specific areas or places and to remain at his residence for specific periods of time. Abidance is controlled by means of electronic monitoring. If the convict released on parole leaves the allowed area, his parole officer is notified via sms.[158] The Data Protection Commissioner of Hesse voiced the

---

[154] Spiegel Online, Die Polizei, Dein Freund und Datensammler, 5 March 2007. Available at: <http://www.spiegel.de/netzwelt/tech/0,1518,465388,00.html>.
[155] Landesverwaltungsgesetz Schleswig-Holstein (LVwG-SH).
[156] Heise Online, Elektronische Fußfessel – Die Zahlen, 29 April 2005. Available at: <http://www.heise.de/newsticker/meldung/59130>.
[157] Strafgesetzbuch (StGB). Available in German at: <http://www.gesetze-im-internet.de/stgb/BJNR001270871.html>. Article 56 lit. c StGB reads: 'The court shall issue instructions to the convicted person for the duration of his term of probation, if he requires such assistance to cease committing crimes. No unreasonable demands should thereby be made on the way the convicted person conducts his life. In particular, the court may instruct the convicted person to follow orders which relate to residence […].'
[158] State of Hesse Ministry of Justice, Sicherheitsland Hessen – Elektronische Fußfessel im praktischen Einsatz, November 2003. Available at: <http://www.justiz.hessen.de/C1256FF500438727/CurrentBaseLink/A82A1171CA151894C1256FF1004B3CA0/$File/Vortrag_Fussfessel%20aktuell.pdf>.

opinion this current statutory basis was not sufficient.[159] He argued electronic monitoring was comparable with supervision of conduct as laid down in Article 68 Criminal Code[160]. The Commissioner therefore called for the introduction of a specific legal basis covering electronic monitoring.

A further law dealing with the location of citizens are the Registration Acts of the German states. German citizens are obliged to notify the municipal registration office if they change their permanent residence. The registration office keeps records which among other data hold the name of the citizen and the present and former address of his domicile. This kind of general localisation of property belonging to an identifiable person is not in the focus of this report, which looks into provisions concerning the actual whereabouts of a person at a specific point in time.

7.4 Legal framework for processing location data by private parties

The Telecommuncations Act and the Telemedia Act apply only to generating and use of location data by telecommunications service provider and telemedia service provider. If a private party wants to generate or use location data of a third party, a statutory basis is required. As no specific law applies the regulations of the Federal Data Protection Act must be complied with. In particular, the requirements laid down in Art. 28 BDSG[161] must be met. In addition, other legal bases or jurisdiction may have to be taken into account.

7.4.1 Electronic monitoring of employees

A growing use of LBS can be observed in workplace environments. If employees and working appliances are not necessary bound to one fixed workplace, coordination of employees' changing job sites becomes more important. Fleet management aims at effective coordination of employees and by means of saving of time and expenses increase efficiency. Localisation of employees can also bring about advantages for the employee who will not have to engage in planning, coordination and controlling as these tasks can be taken over by a centralized organisation department.

At the same time generating and use of employees' location data allows monitoring of performance, behaviour, and contextual information (where does the employee spend his lunch break; does he visit a specific doctor etc.) and linking this information enables behavioural profiling. The employee can be subjected to permanent surveillance.

---

[159] 31st annual report of the Data Protection Commissioner of Hesse, 31 December 2002. Available at: <http://www.datenschutz.hessen.de/TB31/K23P03.htm>.

[160] Article 68 StGB reads: 'If someone has incurred a fixed term of imprisonment of at least six month for a crime, in relation to which the law specifically provides for supervision of conduct, then the court may order supervision of conduct collateral to the punishment if there is a danger that her will commit further crimes.'

[161] Article 28 BDSG reads: ‚The collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes shall be admissible (1) in accordance with the purpose of a contract or a quasi-contractual fiduciary relationship with the data subject, (2) in so far as this is necessary to safeguard justified interests of the controller of the filing system and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use, (3) if the data is generally accessible or the controller of the filing system would be entitled to publish them, […]'.

In this context the employer's right to lead his business and the employee's right to informational self-determination are affected. As a general rule, the employer has the duty of care for his employees.

Applying the description of legal requirements for the provision of Location Based Services (see 2.3) to fleet management leads to the following first findings: in the context of fleet management a four-sided relation exists. The employer who contracts to the provision of LBS is subscriber to the telecommunications service and the driver of the positioned vehicles is the user of the telecommunications service. The role of the telecommunications service provider and the content provider remain unchanged. As the provision of a LBS requires data which is not anonymized, consent of the subscriber (the employer) is necessary. Consent of the user (the employee) is not required but the subscriber is obliged to inform the co-user of all such given consent.

When contracting to fleet management the employer is not entirely free to decide about generation and use of location data relating to his employees. He is bound by obligations deriving from the labour contract. In Germany the introduction of a specific employee data protection law has long since been demanded. Until today no specific regulation exists and so jurisdiction has established binding principles instead.

The introduction of location based fleet management must comply with the requirements laid down in Art. 28 BDSG.[162] If the content provider and the employer enter a contract and lay down a specific purpose which requires generating and use of employee's personal data (including location data), the use of employees' location data is admissible.

Furthermore, Art. 87 paragraph 1 lit.6 Betriebsverfassungsgesetz (BetrVG) must be complied with. This provision requires involvement of the company's works council (*Betriebsrat*) if the 'introduction and use of technical equipment aiming at monitoring employees' behaviour and performance is planned'. Employer and works council shall close a company agreement (*Betriebsvereinbarung*) protecting the employees' personal rights, Art. 75 paragraph 2 BetrVG. This company agreement shall follow the trade-off laid down in Art. 28 BDSG. The introduction of LBS is therefore only admissible if necessary and reasonable to safeguard a legitimate purpose.

7.5 Conclusion

The legal provisions covering the use of location data in Germany are complex and cover the Telecommunications Act, the Telemedia Act and the Federal Data Protection Act. Directive 2002/58/EC was transposed into national law by amending the Telecommunications Act.

The following figure presents the steps of data processing which occur during the provision of a LBS:

[162] Hallaschka F. & Jandt S. 2006. Standortbezogene Dienste im Unternehmen, 2006.

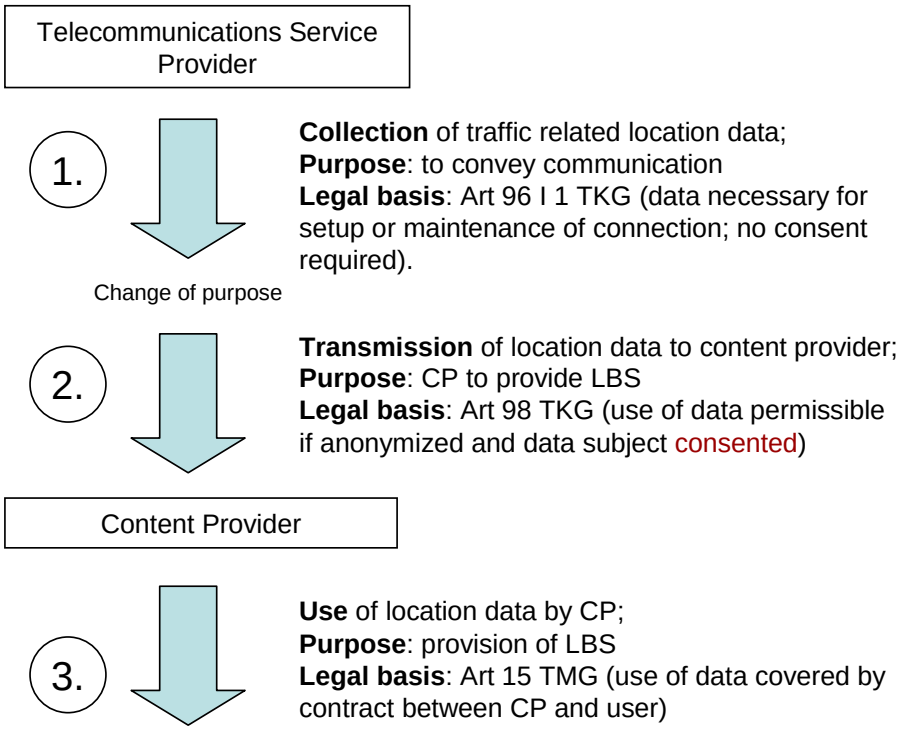

Figure 9: Processing of location data and legal bases

While it has been argued that as consent is obligatory at the stage of collection of location data by the telecommunications provider, the lack of a second obligation to obtain consent for the content provider does not lever out the right to informational self-determination, this view has been questioned. A reactive LBS needs to be initiated by an explicit request of a service each time it is needed. This is not the case for a proactive LBS which, if requested once, may lead to permanent monitoring of the cell phone location. Considering the above illustrated requirements, the following gap is apparent: the person originally requesting the LBS and the later user of the cell phone can be two different persons. For example an employer could issue cell phones to all employees or a wife could let her husband use a cell phone she subscribed for. The subscriber (or a different person who secretly uses the phone for a short period of time) or the user can request localisation of the cell phone without the other parties' knowledge and consent to the localisation at "step 2" (transmission of location data to content provider for provision of LBS). Information must be provided at the beginning of the use on the kind of data collected and used, the scope of data collected and used and purpose of data collection and use. But if the requested location based service is a proactive service, localisation spans long periods of time.

Many content providers do not repeatedly send information on the aforementioned indications in irregular intervals and misuse is therefore possible. A regularly obtained consent for proactive location based services would reduce the lack of transparency, at least regular notification should be mandatory.

For public parties, especially law enforcement authorities, location data is of substantial interest when investigating into criminal acts. While some provisions allow for the generation of location data by public authorities, statutes also allow access to location data available at private parties. Access to precise location data collected and processed by Telecommunications Service Providers and Content Providers (see 2.2.1) is not possible for

public parties as it must be deleted when no longer necessary for the provision of the LBS. Traffic related location data on the other hand is treated as traffic data and will following the transposition of the data retention directive be stored for 6 months. For conclusions on preferences, this information can be sufficient. If linked with further traffic data, social networks can be determined.

8 Location Information from a Dutch Perspective

Colette Cuijpers, Bert-Jaap Koops & Arnold Roosendaal (TILT)

8.1 Introduction

In this chapter, we will discuss the Dutch legal framework regarding location data in the context of the provision of location-based services (LBS). After outlining the general legal framework, we will zoom in on a particular issue, namely the conditions for accessing location data by public parties (in particular law enforcement authorities) and by private parties (in particular employers).

8.1 Legal framework: general principles

In the Netherlands the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*,[163] hereinafter: PDPA) is the general law regarding processing of personal data. Similar to the European Privacy Directive (95/46/EC), of which the PDPA is the Dutch implementation, this law applies to all cases except when they are superseded by specific provisions from other laws. One such case concerns the specific provisions for traffic and location data. The provisions of this Directive are implemented in the Dutch Telecommunications Act (*Telecommunicatiewet*,[164] hereineafter: DTA), as adapted by Directive 2002/58/EC.

For the applicability of these acts, the distinction between telecommunications traffic data[165] and location data is of importance. In this report, the focus is on Location Based Services and, thus, location data. However, it should be noticed that some traffic data are also location data. A further distinction has to be made between location data or traffic data which are necessary for billing purposes and interconnection services, and those that are not, because these are excepted from the general rule that processing is only permitted on the basis of consent. (Article 11.5a (2) and 11.5a (3) DTA).

The PDPA is the general law that applies to processing of personal data. If there is a legal ground for the processing of personal data, the PDPA prescribes certain conditions that have to be taken into account. Personal data shall be processed in accordance with the law and in a proper and careful manner (art. 6) and personal data shall be collected for specific, explicitly defined and legitimate purposes (art. 7). These are general conditions that have to be fulfilled if there is a legal ground for the processing. In addition article 9 restricts the processing to the purposes for which the personal data have been obtained, and the data shall not be stored for any longer than is necessary for achieving these purposes (art. 10 (1)).

The first question that arises is what "personal data" are. The PDPA gives a definition in art. 1(a):

> "a. 'personal data' shall mean: any information relating to an identified or identifiable natural person".

[163] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens). All Dutch legislation can be found at <http://www.wetten.nl>.
[164] Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie, (Telecommunicatiewet).
[165] See above, note 1.

This definition is the same as in the Data Protection Directive (95/46/EC). However, the scope of "identifiable" remains a difficult issue and needs to be judged on a case to case basis. The Explanatory Memorandum at the PDPA[166] gives guidelines on how to assess whether or not a person is identifiable. There are two main factors that have to be taken into account: the kind of data and the ability of the controller to accomplish the identification. With respect to the kind of data reference is made to art. 2 (a) of Directive 95/46/EC. This provision mentions *"factors specific to [the] physical, physiological, mental, economic, cultural or social identity"* of the data subject. Furthermore, there is a distinction between directly and indirectly identifying data. 'Directly' means that the data are that unique to a particular person that, in general, with certainty or to a large extent of probability, this person can be identified. 'Indirectly' means that, under certain circumstances, data can be related to a specific person. This result may also be achieved with comparison or connection of data.

The second main factor is the ability of the controller to accomplish the identification. To judge this factor there are no absolute measurements. Guideline is to look at all the tools or devices that may reasonably be assumed to be available to the controller or any other person to accomplish the identification.[167] This means that the ability depends on the function of the controller. For example, a policeman who has access to several (inter)national databases and who has specific legal competences to retain certain data will have more tools to identify a person than a civilian has.

Because of this second factor, it should be noted that technological development may have the consequence that certain data which are not considered to be personal data now, can be personal data in the future. New devices may offer the possibility to make the connection to a natural person. For this report, it is of importance that location data and traffic data can be personal data, as is shown in the general legal chapter (section 4.4).

8.2.1 Processing of location data for the provision of Location Based Services

With regard to the processing of location data for the provision of Location Based Services the Telecommunications Act is applicable. In this Act the provisions regarding traffic data and location data of Directive 2002/58/EC are implemented. Article 6 of the Directive is implemented in article 11.5 of the Telecommunications Act and article 9 of the Directive in article 11.5a of the Telecommunications Act. These provisions cover processing of location data and traffic data by providers of public communications networks or publicly available electronic communications services.[168]

Article 15 of the Directive is implemented in article 11.13 of the Telecommunications Act. The Explanatory Memorandum on the implementation of the Directive in the Telecommunications Act mentions the derogations on the scope of rights and duties of some provisions of the Directive.[169] In this respect also article 5 of the Directive is mentioned on the confidentiality of the communications. However, the same Explanatory Memorandum

---

[166] Memorie van Toelichting Wet Bescherming Persoonsgegevens, Tweede Kamer, vergaderjaar 1997-1998, 25982, nr.3, p.47.
[167] Idem, p. 48.
[168] A significant detail: in the official Dutch translation of Directive 2002/58/EC, available at <http://eur-lex.europa.eu/LexUriServ/site/nl/oj/2002/l_201/l_20120020731nl00370047.pdf> , in article 9 the word 'openbaar' (public) is missing.
[169] Explanatory Memorandum, Tweede Kamer, vergaderjaar 2002-2003, 28 851, nr.3, p.165.

states, with regard to article 5, that further research is needed and that the article will not be implemented so far.[170] At this moment there is no implementation of article 5 in the Telecommunications Act. However, this does not imply that there is no regulation on the confidentiality of communications in the Netherlands. Article 13 of the Dutch Constitution (Grondwet) provides a general right on confidentiality of communications.[171]

8.2.1.1 Purpose specification and proportionality

According to article 11(1) of the PDPA, personal data shall only be processed where, given the purposes for which they are collected or subsequently processed, they are adequate, relevant and not excessive. In addition, article 7 states that personal data shall be collected for specific, explicitly defined and legitimate purposes. With a focus on location data, these purposes can be found in the Telecommunications Act. Processing is allowed for billing purposes and for the provision of value added services. For other purposes processing is only allowed after the data are being made anonymous or with consent of the subscriber or user. (11.5a (1) and (3) DTA) The Dutch definition of 'consent' can be found in article 1(i) of the Dutch Personal Data Protection Act and is exactly similar to the definition in article 2(h) of Directive 95/46/EC.[172]

8.2.1.2 Processing for billing purposes

Providers of public electronic communications networks have the opportunity to process traffic data of subscribers for billing purposes. Article 11.5(2) of the Telecommunications Act states that:

> "The provider may process traffic data necessary for the purpose of subscriber billing, including drafting a bill for a subscriber or a person who has legally bound himself to the provider to pay the bill, or for the purpose of interconnection payment. The processing of traffic data is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued."

This provision is the implementation of article 6(2) of Directive 2002/58/EC with some information added. The added information is the explanation that subscriber billing includes drafting bills for subscribers and for other persons who legally bound themselves to pay the bill. In fact, this only seems to be an example that is covered by the term "billing purposes" in the Directive. The Dutch provision does not seem to have a different scope than is prescribed by the Directive.

8.3 Legal framework for processing location data by public authorities

This section describes situations in which public authorities have access to location data. Besides, it gives a description of the Dutch view on data retention.

8.3.1 Access to location data by law enforcement

There are several investigation powers in the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*, hereinafter: DCCP) that law-enforcement agencies can use to access location data.

---

[170] Idem, p. 46.
[171] Tweede Kamer, vergaderjaar 2001–2002, 27 591, nr. 4, p.4 (under 8).
[172] Article 29 Working Party, Opinion 5/2005 on the use of location data with a view to providing value-added services, WP 115, p. 6.

Requesting location data that are traffic data

The most specific provisions relate to location data that are also telecommunications traffic data. These can be requested of telecom providers, and have to be provided by these in real-time, on the basis of:

- Art. 126n DCCP: the public prosecutor can order the production of traffic data in cases of fairly serious crimes (carrying a maximum punishment of four years or more);
- Art. 126u DCCP: the public prosecutor can order the production of traffic data in cases of fairly serious organised crime, even if not yet committed;[173]
- Art. 126zh DCCP: the public prosecutor can order the production of traffic data in cases of 'indications' of a terrorist crime, i.e., without probable cause (in Dutch: *redelijke verdenking*);
- Art. 126hh DCCP: the public prosecutor can, with approval of the investigating judge, order the production of (parts of) databases, including databases of traffic data,[174] in cases of an exploratory investigation (*verkennend onderzoek*) with the aim of preparing an investigation into serious, organised terrorist crime; he can also combine these data with other databases for data-mining.[175]

The traffic-data in all of these powers include cell-ID data, i.e., the location of the cell of origin and the cell of destination of a call (if these are processed by the telecom provider). They exclude, however, location data generated by mobile phones in standby mode.[176] The location data of phone calls (including sms messages etc.) can be requested, however, for each time the user uses his mobile phone, even if this means that 'heavy users' can thus be virtually tracked throughout their movements.[177]

It is important to note that these powers traditionally could only be used with respect to public telecommunication providers. However, since September 2006, when the Computer Crime II Act entered into force,[178] the powers also can be executed against private telecom providers. The addressees are now defined as providers of communication services, i.e., 'a natural person or legal person who in the course of profession or business offers to users of his service the possibility of communicating with a computer, or who processes or stores data on behalf of such a service or the users of that service' (art. 126la DCCP). This power to request locational traffic data on the basis of art. 126n DCCP is being used more and more in practice; it is generally accepted in case-law that call-related location data are part of traffic data.[179]

For the purposes of this study, two interesting cases are worth mentioning from jurisprudence. The first is the 'Deventer murder case', in which someone was convicted partly on the basis of the location of the call he made very shortly before the murder took place. The call was processed by a base station in Deventer, and the court concluded that the suspect therefore must have been in or near to Deventer at that time, rejecting his contention that he was driving

---

[173] This power was created in 2000 by the Special Investigation Powers Act (*Wet bijzondere opsporingsbevoegdheden*), *Staatsblad* 1999, 245.
[174] Draft Explanatory Memorandum to Telecommunications data retention Bill, note 193, p. 15.
[175] The latter two powers were created on 1 February 2007 with the Extension of the Investigation and Prosecution of Terrorist Crimes Act (*Wet verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven*), *Staatsblad* 2006, 580.
[176] Parliamentary Proceedings Second Chamber [*Kamerstukken II*] 2001/02, 28 059, No. 3, p. 8.
[177] Ibid., p. 8-9.
[178] Computer Crime II Act (*Wet computercriminaliteit II*), *Staatsblad* 2006, 300.
[179] See, e.g., Dutch Supreme Court (*Hoge Raad*) 7 September 2004, LJN-No. AO9090.

on a highway at a considerable distance when he made the call, and that due to special 'atmospheric circumstances' the call must have been received at the distant Deventer base station.[180]

In the second case, the public prosecutor was barred from prosecution (the furthest-reaching sanction by a court) because the prosecution had failed to request traffic data from telecom providers, despite repeated requests by the suspect's attorney to do so. She argued that the locational traffic data of the suspect's mobile phone would confirm his alibi, and she had warned the prosecution that traffic data would only be stored by telecom providers for at most 6 months. When the prosecution finally requested the traffic data, they had already been deleted. Therefore, the court argued that the public prosecutor had grossly neglected the interests of the defense.[181] This case shows that data retention of location data may also be usable as disculpatory evidence.

Requesting location data that are not traffic data

For location data that are not traffic data, e.g., the location data of mobile phones in standby mode (provided the telecom provider stores these), the public prosecutor can also order the production to telecom providers, on the basis of art. 126ng DCCP (fairly serious crime), 126ug DCCP (planned serious organised crime) or 126zo DCCP (indications of terrorist crime). If others than telecom providers store such location data, the prosecutor can use the general production order, art. 126nd DCCP (fairly serious crime), 126ud (planned serious organised crime), and 126zl DCCP (indications of terrorist crime).

These data should not be sensitive data, e.g., relating to religion, health or sexual life; if there is reason to assume that ordered location data would reveal sensitive locations, e.g., visits to a church, venereal-disease clinic, or gay cruising area, the public prosecutor needs the approval of the investigating judge and should use the more stringent provisions for ordering sensitive data (artt. 126nf, 126uf, 126zn DCCP).

Search and seizure

Instead of ordering the production of data, law enforcement can also search and seize such data. The main relevant provision here is art. 125i DCCP, which allows law-enforcement authorities to search places with the aim of copying data. Depending on the sensitivity of the place, a higher authority is needed; e.g., only an investigating judge can search a dwelling (art. 125i j^{o} 110 DCCP), whereas all investigation officers can search vehicles (art. 125i j^{o} 96b DCPP). Lower authorities can execute search and 'seizure' (or copying of data) for more serious crimes, but the investigation judge can search and 'seize' in all crime cases.

---

[180] Court of Appeal (*Gerechtshof*) Arnhem 22 December 2000, LJN-No. AD8964. See also consideration 15 of the conclusion by the advocate general in the appeal for cassation, which the Supreme Court denied on 20 November 2001, LJN-No. AD5148. The case has a rather bizarre subsequent history of revision and re-conviction (and a privately detecting reporter accusing another citizen of the murder), see <http://www.rechtspraak.nl/Actualiteiten/Dossiers/Deventer+moordzaak.htm>. The contentious location data were at length discussed by the Court of Appeal 's-Hertogenbosch 9 February 2004, LJN-No. AO3222, section 2.3, and the Court concluded that the suspect must have been in or near Deventer, basing themselves on testimony of four experts.

[181] District Court (Rechtbank) Rotterdam 5 September 2006, *Nieuwsbrief Strafrecht* 2006, No. 449.

8.3.2 Access to location data by national-security agencies

The powers of the General Intelligence and Security Agency (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) and the Military Intelligence and Security Agency (Militaire Inlichtingen- en Veiligheidsdienst, MIVD) are regulated in the Intelligence and Security Agencies Act 2002.[182] Art. 28 gives both agencies the power to order telecom providers to produce traffic data, similar to the law-enforcement power of art. 126n DCCP (see above). For this, no authorisation is needed. There is no description of the cases in which the agencies can do this, except that it 'must be necessary for the good execution of their task' (art. 18); also, there is a general proportionality requirement (art. 31).

Moreover, a bill is considered to give the agencies also a power to request (parts of) databases from telecom providers for data-mining purposes, upon authorisation of the relevant Minister.[183]

For location data that are not traffic data or stored by others than telecom providers, the agencies can use a general power to ask for (presumably voluntary) production of data (art. 17); they can also search places and, if necessary, seize goods (art. 22) or hack computers, e.g., of telecom providers (art. 24).

8.3.3 Access to location data by other public authorities

The General Administrative Law Act (*Algemene Wet Bestuursrecht*[184]) provides some powers for supervising authorities to access data. However, in relation to location data this is rather far-fetched, so this will not be discussed further in this chapter.

8.3.4 Electronic bracelets

In the Netherlands, some applications of electronic bracelets exist. For example, since 2003 electronic detention is possible. The person who has been convicted has to wear a bracelet and stay at home. The bracelets are provided with a GSM system connected to the home telephone[185] of the persons wearing them.[186] The restriction to the home environment is the sanction and is considered to be a lighter form of detention than detention in a prison. It is meant only for persons with a detention period of 90 days maximum.[187] If the person leaves his home, or his working area to which he can also be authorized, a signal is given to supervisors and they can come into action. The considerations in favour of electronic detention are the ability to continue family life and work. Reintegration in society is the main objective. Besides, because of the lack of need for intensive supervision, costs of detention

[182] Intelligence and Security Agencies Act 2002 (*Wet op de inlichtingen- en veiligheidsdiensten 2002*), *Staatsblad* 2002, 148.
[183] Draft Explanatory Memorandum to Telecommunications data retention Bill, note 193, p. 16.
[184] Wet van 4 juni 1992, houdende algemene regels van bestuursrecht (Algemene wet bestuursrecht) Stb. 1992, 315.
[185] WODC 2005. Geboeid door de enkelband, Evaluatie pilot Elektronische Detentie, Nijmegen: ITS, 2005, p.45
[186] See: <http://www.pizuidoost.nl/roermond/elektronischedetentie/ed.htm>.
[187] See: <http://www.postbus51.nl//index.cfm?vid=4568FCD9-1635-38D4-CF08FEFCC499F190&containerid=517415FF-C09F-296A-61FF669427684C44&objectid=DA341909-1635-38D4-CF5217E2AC796504&displaymethod=displaydefaultintro>.

are diminished. These arguments have been discussed in parliament[188] as well as in academic studies.[189]

With regard to detention during her Majesty's pleasure (in Dutch: *TBS*, *Terbeschikkingstelling*) there have been some experiments using GPS. Within the Dutch legal system, TBS is a period of time during which a person is detained under the scrutiny of legal, medical or social order. The TBS system ensures professional guidance for detainees and offers supervised reintegration into society. In order to obtain this objective, there are releases on parole. During the release, the detainee wears a bracelet with a GPS sensor. However, the experiments have not been successful so far, because the sensors can be shielded to easy with, for example, aluminium foil. Another problem lies in the accuracy in urban territories.[190]

The safety of the system is subject to discussion, because of some cases of escaped detained persons, who then committed new crimes, during the last months. However, new experiments will be launched soon.[191]

8.3.5 Mandatory data retention of location data

Even before the EU discussion and the consequent Directive on Data Retention, the Netherlands had created an obligation, with a limited scope, for telecom providers to store traffic data, including location data. The reason for this is that it is impossible to wiretap someone who uses prepaid cards, for lack of a known number to tap. To address this problem, article 13.4 (2) of the 1998 Telecommunications Act stipulated that telecom providers have to store traffic data for a period of three months. The data to be stored are listed in an Order in Council, which was enacted only as of 1 March 2002.[192] The data listed are time, number, and cell-ID. Through the cell-ID, the location of a mobile telecommunication therefore has to be stored for three months.

To implement the Data Retention Directive, a draft Bill was published in January 2007, which would alter the Telecommunications Act and the current, limited, data-retention provision.[193] Art. 13.4 would now be extended to require all telecommunication providers to store the traffic data as designated in an Order in Council for a period of 18 months. These data would include not only the location of the cell of origin and the cell of receipt of mobile telecommunications, but also the location of any other cell during the communication.[194] The draft Bill has triggered critical reactions not only by the telecommunications industry,[195] but also by the Dutch Data Protection Authority. The latter argued that the 18-month retention period was unsubstantiated and should be changed to the European minimum period of 6 months, and that no retention should be required of location data generated *during* a call,

---

[188] Kamerstukken II, Tweede Kamer, vergaderjaar 2004–2005, 29 800 VI, nr. 167, p.2.
[189] WODC / ITS Nijmegen 2005. Geboeid door de enkelband: evaluatie pilot elektronische detentie, Nijmegen 2005.
[190] See for example: <http://www.goedzo.com/index.php/2005/12/10/proef_gps_enkelbanden_tbs_ers_mislukt>.
[191] See: <http://www.nu.nl/news.jsp?n=932166&c=13>.
[192] Decree on special collection of telecommunications number data (*Besluit bijzondere vergaring nummergegevens telecommunicatie*), *Staatsblad* 2002, 31.
[193] Draft Telecommunications data retention Bill (*concept Wet bewaarplicht telecommunicatiegegevens*), available at <http://www.justitie.nl/images/5454571%20Wet%20cons_tcm34-31070.pdf>. Cf. the Ministry of Economic Affairs' consultation website: <http://www.minez.nl/content.jsp?objectid=149504&rid=144530>.
[194] Draft Explanatory Memorandum, ibid., p. 4.
[195] Letter on the Data-retention Bill consultation, 18 January 2007, available at <http://www.xs4all.nl/opinie/wp-content/uploads/2007/gez_reactie_aanbieders_wetsvoorstel_dataretentie.pdf>.

since this would enable *'an all too intrusive, comprehensive secret surveillance of the movements of very large numbers of unsuspected citizens'* (our translation).[196]

8.4 Legal framework for processing location data by private parties

For the provision of value-added services access to location data by private parties can be allowed as already discussed in the general legal chapter. In section 8.4.1 the use of location data in an employer-employee relationship within the Netherlands will be discussed. Section 8.4.2 gives some brief examples of other applications in the Netherlands in private relationships.

8.4.1 Privacy in an employee employer relationship

As described in the general legal chapter privacy and processing of personal data in an employment relationship leads to specific questions. How do the privacy legislations apply in a working sphere? Can an employee trust on privacy during working time, when using devices from his employer? Or if he uses a car from his employer with a GPS system built in, can he reasonably expect that his employer will not use the location data in order to control work efficiency? And are there important differences between a working sphere and requests for location information from other private parties, not being an employer?

8.4.1.1 Traffic data in the employee employer relationship

In an employee employer relationship it can be justifiable for an employer to check e-mail and internet use of his employees. The Dutch Data Protection Authority has published a report, "Working well in networks"[197], in which guidelines are provided on how to check e-mail of individual employees. It states that logging can be used, but should be restricted to traffic data as much as possible. By using traffic data (sender, receiver, date, time and destination) it is possible to forward messages to the right department or person. Further details and content of the communication are, in general, not necessary and should be avoided. Furthermore, it is recommended that traffic data are only processed and stored as long as necessary for the aim of processing.

8.4.1.2 Case law specific to the employee employer relationship

In the Netherlands there is a lot of case law concerning Internet and e-mail monitoring and camera surveillance in the workplace. So far, there are only few cases concerning localisation of employees. However, from the few cases, it can be concluded that the same reasoning will apply as is the case with regard to internet, email and camera surveillance. At least there has to be knowledge by the employee that he can be monitored or watched. In a recent case the court considered that monitoring employees with cameras is permitted and that the use of hidden cameras is permitted in certain circumstances on the condition that the employees are being informed about this possibility on forehand.[198]

---

[196] Letter on the Traffic data retention implementation Bill, 22 January 2007, available at: <http://www.cbpweb.nl/documenten/adv_z2006-01542.shtml?refer=true&theme=purple>.
[197] Terstegge J.H.J. 2002 (CBP). Goed werken in netwerken, Achtergrondstudies en verkenningen 21, Den Haag, april 2002, p.38 (available at: <http://www.cbpweb.nl/downloads_av/av21.pdf?refer=true&theme=purple>).
[198] Rb. Haarlem sector kanton, 24 mei 2006, 309644 / VV EXPL 06-113.

In a recent case the Court considered it to be lawful that an employer compared daily working reports of an employee with the print out of the GPS system. Because of the big discrepancy between these both documents, the employer was allowed to terminate the employment contract.[199] In another case, a GPS provider had to disclose GPS data from a car that had been involved in an accident to enable the police to verify the speed of the car at the moment of the crash.[200] However interesting, this case was not specifically related to a private relationship.

In general, the problem remains that article 11.5a (3) of the Telecommunications Act requires necessity of the processing of location data to provide a value added service. In the occasion of mere monitoring of employees, there is in fact no value added service, so in general this way of monitoring is prohibited, unless there is a prior informed consent of the individual data subject (11.5a (1) DTA). To obtain prior informed consent of each data subject individually might be difficult. For larger companies, a remedy for this problem is offered in the Dutch Works Council Act.[201] According to article 27 of this Act, the employer needs the works council's consent when he intends to implement, alter or withdraw rules on the processing of employees' personal data.[202] However, the fact that certain employees or the Works Council have agreed with (camera) surveillance does not imply that the surveillance cannot be unlawful against employees.[203] It can only be an indication that the employer has a justified interest in the surveillance.[204] In addition, it should be noted that the agreement of the Works Council does not replace the individual consent of the employees.[205]

8.4.1.3 Location data directly available for the employer

In the above the starting point was that the location data had to be obtained from a third party, the provider. However, it is also possible that data are generated by internal systems which are directly accessible for employers. In this context examples are access verification systems based on RFID or biometrics or chip card systems for internal use.

If the employer has immediate access to location data the question arises if the use of these data is allowed and, if so, under which circumstances. In general the same rules apply as to the data collected by third parties. The use of data, directly available or not, implies processing of these data. That means that there has to be a legitimate ground for the processing like set out above.

In the Netherlands there is an obligation to register data processing with the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*, hereinafter: CBP) or with a special privacy officer for an organisation or branch. In general, this also counts for data of

---

[199] Smits D. 2006. Exit-route via GPS?, 23 oktober 2006, see: <http://www.expertlog.nl/2006/10/exitroute_via_g.html>.
[200] Veldhuijzen A. 2006. Autocomputer is ook bewijs, 20 oktober 2006, see: <http://www.ad.nl/autowereld/article730043.ece>.
[201] Wet op de Ondernemingsraden (WOR) of January 28th 1971, *Stb*. 54, last amendment on 18th of March 1999, *Stb*.184.
[202] Hendrickx F. 2005. Privacy and Data Protection in the Workplace: The Netherlands, in: Nouwt S., DeVries B.R. & Prins C. (Eds.), Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, The Hague: TMC Asser Press 2005.
[203] Hof 's-Hertogenbosch 2 July 1986, NJ 1987,451 (KOMA), r.o.4.4.
[204] Koevoets M.M. 2006. Wangedrag van werknemers; De bevoegdheid van werkgevers tot opsporing en sanctionering, dissertation, Den Haag: Boom Juridische Uitgevers 2006, p.39.
[205] See: <http://www.cbpweb.nl/downloads_inf/inf_va_personeelsgegevens_derden.pdf?refer=true&theme=purple>.

employees. However, some standard processing is excluded from this obligation. Most personnel and salary administrations and some employee monitoring systems fall into the exclusion. The Exemptions Decree (*Vrijstellingsbesluit*) gives the situations and requirements for the exemption. Only if all requirements are met, processing is exempted from the duty to register. The decision whether or not to register lies with the employer himself, in accordance with the Works Council.[206] However, the Dutch Data Protection Authority supervises the system of registration.

As mentioned in the general legal chapter, it is questionable whether internal systems, which are directly accessible for employers without the involvement of a third party, fall within the scope of directive 2002/58/EC as these systems may not qualify as 'public'. In the Netherlands the requirement of 'public' has been implemented into the Telecommunications Act, meaning that also in the Dutch legal system the articles 11.5 and 11.5a DTA do not apply to non-public communications networks and services. As the term 'public' is not defined, it is unclear which communication techniques fall within the scope of these articles.

Some branches have adopted Codes of Conduct with regard to processing of personal data.[207] Companies with their activities in one of these branches can be subject to these Codes of Conduct. These codes can contain specific clauses regarding the processing of personal data of employees.

8.4.2 Other private applications in the Netherlands

8.4.2.1 GPS

With regard to location data and GPS the Dutch government proposed a legal obligation for tracking and tracing of transport of fertilizers in the Meststoffenwet (Fertilizations Act). For the sake of environmental protection the proposed system would allow monitoring of amounts and volumes of fertilizers that are transported. The CBP has stated that there was no discussion that the execution and enforcement of the Fertilizers Act, and the orders in pursuance of the Act, regarded for a substantial part the processing of personal data, and, thus, the PDPA should be applied.[208]

The CBP concluded that the use of a GPS system to track fertilizers transport leads to a detailed administration which will be used to check the transports and volumes. However, these data are connected to natural persons. In this respect, the proposed obligations imply an infringement of the personal privacy for which the necessity has not been clarified properly.

In 2006, the Minister of Agriculture, Nature and Quality of Food, decided in the evaluation of the Fertilizations Act that he would make an exception to the obligation for GPS monitoring. However, this decision was based on economical considerations; the costs to imply the systems were too high, so it was difficult for the Netherlands to compete with other countries.[209]

---

[206] Terstegge J., Zijn uw systemen WBP-proof?, available at: <http://home.planet.nl/~privacy1/wbpproof.htm>.
[207] For an overview of approved codes of conduct see: <http://www.cbpweb.nl/indexen/ind_wetten_zelfr_gedr.shtml?refer=true&theme=purple>.
[208] CBP, Advies wetsvoorstel wijziging Meststoffenwet, 3 november 2004.
[209] Evaluatie Meststoffenwet, Tweede Kamer, vergaderjaar 2005-2006, 28 385 en 30 252, nr.73.

However, it can be concluded that if tracking and tracing of transports with GPS raises privacy concerns with the CBP, tracking and tracing of persons as such (e.g. employees) will certainly raise main concerns.

8.4.2.2 Bluetooth

Another technology interesting to mention is Bluetooth. In the Netherlands there have been some uses of Bluetooth for advertisement purposes. Some companies used Bluetooth to send promotional messages and movies to passers-by. People who had the Bluetooth function on their cell phone turned on received the messages. There is discussion[210] if this type of advertising can be considered to be spam. In the Netherlands, the OPTA (Independent Mail and Telecommunications Authority) has to enforce the spam prohibition and to supervise the telecommunications sector. This means that, with regard to telecommunications, in the Netherlands two authorities, CBP and OPTA, are involved to supervise processing of data.

Also in this discussion the definition of public telecommunications networks is important. For now, the OPTA considered advertisements transmitted through bluetooth not to fall within the scope of the definition of spam, because the messages were sent to anyone who passed by, regardless of them being a subscriber to the service or not.[211] However, they call on all people who received unsolicited messages to complain.

8.4.2.3 WiFi

A quite similar discussion counts for WiFi. WiFi can be considered to be an electronic communications network and an electronic communications service. However, questions arise in relation to the term 'public'. The WiFi technology in fact provides only a connection, as a mere transfer point, between a service provider and a user. It is only the technology of a wireless connection. The public service lies not in this system, but with the original service provider, such as an ISP.[212] As a result, the WiFi services are not subject to the Telecommunications Act and its related obligations, such as registration with the OPTA and wiretapping facilities. These obligations count for the fixed service provider. However, it is not as clear as it seems to be. The boundary between a public and a non-public electronic communications network lies in the access to the network, not in the service behind it. If the provider of a WiFi network requires registration of its users and works with login codes, the service is not public; not every passer-by can use the network.[213] This implies that a service which is immediately accessible, without registration, should be considered to be public. In this respect, WiFi might be subject to the Telecommunications Act, depending on the circumstances.

8.4.2.4 RFID

With regard to RFID there is also discussion in the Netherlands. Similar to WiFi it can be argued that the Telecommunications Act does not apply, because of the absence of

[210] <http://weblog.ictrecht.nl/reclame/reclame-via-bluetooth-spam/>.
[211] <http://www.planet.nl/planet/show/id=74265/contentid=807253/sc=af2bbd>.
[212] De Jong J.D.C. 2005. Een juridische blik op WiFi, Wetenschapswinkel Rechten, Universiteit van Utrecht 2005, p.16.
[213] Idem, p.17.

subscribers. In general, individual companies will use RFID for several purposes and the consumer, confronted with RFID, is the 'subject' and does not use the technology actively.[214]

However, the CBP takes a different approach to RFID. In a report completely devoted to the RFID technology it states that it cannot be judged yet if the existing legal framework for the protection of privacy is sufficient for the risks of RFID technology. The rules only apply if the data concerned can be labelled personal data, which depends on the use of RFID. Depending on the circumstances this use might imply processing of personal data.[215]

8.5 Conclusion

In the Netherlands, processing of location data is in general regulated by two laws, the Personal Data Protection Act and the Telecommunications Act. These acts implement the provisions prescribed by the European Directives and apply to public as well as private processing of personal data. With regard to use of location data by public authorities, there are some specific provisions in the Dutch Code of Criminal Procedure. There are no specific rules for the processing of location and traffic data within private relationships. However, in employee-employer relationships, the Netherlands offer the opportunity to obtain consent by means of a Works Council. The agreement between the employer and the Works Council cannot replace the consent of individuals, meaning that individual employees can still limit their consent.

The problems described with regard to the complex system of the different European directives being applicable to different types of data (see Chapter 4) are not solved at the Dutch national level. The same holds true for the lack of clarity concerning certain definitions, leaving question open such as "what techniques and services fall within the scope of 'public telecommunications network' or 'public telecommunications service'?" These issues might be hard to clarify at a national level, especially in the Netherlands where two supervising authorities, the CBP and the OPTA, have competencies with regard to telecommunications. On the issue of GSM and GPS there is some clarity, but questions are raised by newer technologies, such as WiFi, Bluetooth and RFID.

In conclusion, the complex system of processing of personal, location data and traffic data is in need of clarification, especially in view of the increasing use of new communication technologies. As long as it remains unclear which provisions apply to different LBS applications under which conditions, the protection of our privacy remains uncertain and the development of LBS may be hampered.

[214] ECP.nl 2005. Privacyrechtelijke aspecten van RFID, mei 2005, p.29.
[215] Beugelsdijk R. 2006. RFID; Veelbelovend of onverantwoord?, CBP oktober 2006, p.33.

9 Conclusions and recommendations

Colette Cuijpers & Bert-Jaap Koops (TILT)

This report aims at identifying legal certainty and privacy protection with regard to positioning systems, in particular Location Based Services (LBS). The main question is:

> Which legal data-protection framework applies when providers of location-based services (LBS), public authorities and private parties like employers process location data generated in positioning systems?

In order to answer this question, this report has provided a description of the technical and the European legal background regarding Location Based Services, as well as an overview of LBS provisioning in relation to the national legal frameworks in four European Member States. In this chapter, we draw conclusions and provide some recommendations on the basis of the descriptions and analyses offered in this report.

9.1 The technical framework

Chapter 3 of this report shows that different kinds of technologies can be used to provide Location Based Services (LBS). The categories of technologies distinguished are:

- Satellite-based positioning systems;
- Sensor-based systems;
- Other wireless technologies, such as Radio Frequency Identification (RFID) based systems or wireless communication systems, such as WiFi or Bluetooth;
- Cell-based mobile communication networks;
- Chip-card-based systems

Since theses technologies differ a lot in the way they work, their characteristics and in their level of accuracy, they are all suitable for different kinds of LBS. Furthermore, there are differences with regard to the limitations and possibilities to disturb or manipulate these positioning technologies. Also the purpose for which location data is intended to be used will be of influence on the technology best suited to provide a certain LBS. As pointed out in the third chapter, location information typically is generated in location systems, which typically consist of two or three types of components:

1. One or more devices sending location information to sensors in case sensors do not operate optically.
2. Sensors to receive and transfer location and time information to static or mobile backend systems.
3. Backend systems interpreting and / or using location information.

In this respect, not only differences exist with regard to the technologies used to provide LBS, but also the parties involved in the process can differ to a large extent. This means that control issues regarding the data that will be generated within these location systems can be complex, as generating and processing of these data in many cases is not done by the same organisation (or data controller).

There are also differences regarding the way in which location and traffic data are generated within these systems. Processing may be done continuously or by request at a certain time. In addition the generation and processing may concern location data of the user of a location system himself, or of another person.

In view of these differences, it is difficult to give a general conclusion regarding the question as to whether the technologies used to provide LBS infringe upon human rights such as privacy. The technologies can offer security functions that provide some guarantees with regard to the fair processing of (personal) location data. However, the effectiveness of these guarantees depends to a large extent on the question whether or not the persons whose data are being processed can use these functions or are allowed to use these functions by the subscribers to the service, such as for example employers. The question as to whether LBS infringe upon personal freedoms such as privacy also depends on the way in which technology is used to provide these services. Besides technical specifications, the law plays an important role. As a general conclusion in view of the technical chapter it can be mentioned that there is a close relationship between technique and law in this respect. The law sets boundaries with regard to the legality of the processing of certain data and can also prescribe minimum (technical) security measures in order to protect human rights. On the one hand technology provides the opportunities to generate and process these data in accordance with the law; on the other hand it also provides opportunities to infringe upon rights guaranteed by law.

9.2 The European legal framework

9.2.1 General rules and principles

From the fourth chapter it becomes clear that the current legal framework regarding the processing of (personal) location and traffic data is very complex, leading to the conclusion that protection of privacy might not be as thorough as it should be.

The main difficulty regarding the European legal framework concerning location data lies with the legal definition and qualification of different groups of data, the overlap that exists between these groups, and the different legal regimes applicable to the different groups of data. The rules regarding the processing of personal data as laid down in Directive 95/46/EC are particularised and complemented with the rules regarding location data and traffic data as laid down in Directive 2002/58/EC. This leaves room for all kinds of combinations between personal, location and traffic data. The different directives lay down different regimes for the processing of the different kinds of data. They are addressed to different parties; they differ in scope; and they contain obscurities with regard to certain definitions. Therefore, it is fair to say that a very complex legal framework for the processing of (personal) location and traffic data is created. Even though the Article 29 Working Party tries to clarify certain issues regarding this complex legal system, still important questions remain. Moreover, it sometimes is questionable whether the opinions of the Article 29 Group are correct, especially in view of the current technological possibilities. For example, with regard to the relation between location data and personal data, the Group claims: *"Since location data always relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in Directive 95/46/EC"*.[216] We consider this too sweeping a statement, since 'location data' in the sense of Directive 2002/58/EC (i.e., indicating the location of a user's terminal equipment) can relate to objects that are not linkable to individual natural persons.

[216] Working Party 29, *Opinion on the use of location data with a view to providing value added services*, WP 115, November 2005, p. 3.

The picture described above becomes even more complicated when assessing whether certain kinds of technologies used to process (personal) location and traffic data fit the definitions of *communication services* and *communication networks* as laid down in Directive 2002/58/EC. From the definitions used within this directive it becomes clear that applicability of the rules is to a large extent technology-dependent.

Whether or not certain data are to be qualified as traffic data mainly depends on the question what is to be understood by *communication* and *electronic communications network* as defined in article 2 of Directive 2002/21/EC. Besides the definition of *electronic communications network*, for the qualification of location data the requirement of *public availability of the electronic communications service* is also of importance. A definition of what is to be considered a communication is given in article 2 (d) of Directive 2002/58/EC. These definitions determine whether the data generated by the various technologies identified in the general technical chapter can be considered traffic and/or location data.

The reason why it is important to be able to determine what data are being processed, relates to the differences that exist with regard to the circumstances under which processing is allowed from a legal perspective. With regard to traffic data the articles 5 and 6 of Directive 2002/58/EC are relevant, prescribing confidentiality, erasure and anonymisation. For location data, other than traffic data, article 9 of Directive 2002/58/EC states that these data may only be processed if the data are made anonymous, or with the consent of the users or subscribers.

The general rules as laid down in Directive 95/46/EC apply to location and traffic data when these data also qualify as personal data. One of the main differences between Directive 95/46/EC and Directive 2002/58/EC relates to the grounds on which processing is allowed. Article 7 of the general Data Protection Directive provides several grounds for the legal processing of personal data. The specific privacy directive only allows processing of location data, and the processing of traffic data for marketing electronic communications services or for the provision of value added services, on the basis of consent.

In principle, the sectoral E-Privacy Directive takes precedence over the general Data Protection Directive. However, the general Directive supplements the protection of traffic and location data when they are not covered by specific provisions in the sectoral Directive. The picture is compounded by the fact that the E-Privacy Directive provisions only apply to *public* communications. Articles 5, 6 and 9 of Directive 2002/58/EC do not cover traffic and location data generated by private networks or in private services. However, if the data can be qualified as personal data and relates to natural persons, the general Data Protection Directive applies.

This demonstrates that many questions need to be answered before it can be determined whether or not what kind of legal regime is applicable to the processing of (personal) location or traffic data:

1. Are the data to be processed ‘personal data’? (see art. 2(a) of Directive 95/46/EC)
2. Are the data to be processed ‘traffic data’? (see art. 2(b) of Directive 2002/58/EC)
3. Are the data to be processed ‘location data’? (see art. 2(c) of Directive 2002/58/EC)
4. Do the data relate to users or subscribers of public communications networks or publicly available electronic communications services? (see art. 6 and 9 of Directive 2002/58/EC and art. 2 (a), (c) and (d) of Directive 2002/21/EC)
5. Is one of the exceptions applicable? (see article 13 of Directive 95/46/EC and article 15 of Directive 2002/58/EC).

9.2.2 Remaining questions

In this respect, without being exhaustive, some remaining questions will be described that are illustrative for the complexity of the legal framework and the problems this creates for its practical applicability. In our view, these issues should definitely be clarified at a European level in order to create a legal framework that provides sufficient guarantees for the protection of human rights in the case of the provision of LBS.

First, it is not certain that location data of a mobile phone in stand-by mode is also needed to be considered traffic data, as it is not clear whether they can be considered to be processed *'for the purpose of the conveyance of a communication'* as is required by the definition of traffic data as laid down in article 2(b) of Directive 2002/58/EC. In stand-by-mode the phone does not process the location data for the purpose of conveying *a specific* communication; it may well happen that there will be no communication at all. The categorisation of 'stand-by' location data is therefore a fairly open issue that Member States have to decide upon when implementing the directive. As the European Legal Framework does not provide guidelines in this respect, Member States might take a different approach towards these kinds of location data.

A second problem relates to the criteria of *'public availability'*. Satellite-based positioning systems and cell-based mobile communication networks in general will be public, in a sense that they are available to the public at large. However, from a technical perspective it is possible, and in view of specific electronic communication services probably already effective, to restrict the access to these networks and services to such a confined group of users that 'public availability' no longer exists, leading to the consequence that Directive 2002/58/EC might no longer be applicable. Also with regard to RFID, WiFi and Bluetooth, a clarification is necessary. As such, these technologies fall within the very wide definition of electronic communications network, since they concern a transmission system to convey signals by electromagnetic means. Often, applications using RFID, WiFi and Bluetooth will also conform to the definition of electronic communications service, if the application can be considered a service. In most cases, these technologies are embedded in some sort of system that can be considered a service, if we go by the general meaning of this term. However, it is questionable whether these technologies need to be perceived as public. On the one hand they are open to everyone who is in its vicinity, but from a geographical perspective the necessity to be in the vicinity of the technical device constitutes a large restriction to the notion of public availability. Whether or not the requirement of public availability will be upheld in the future is questionable as the Article 29 Working Group already pointed at the increasing importance of private networks and the desirability to bring these within the scope of the legal framework as well. This is an important issue as such, as it makes it possible to withdraw LBS from the legal framework by using private means of communications. For example this can be the case with regard to localisation systems used by large businesses in order to track and trace their employees. Because private systems deployed by the employer probably will not qualify as 'public' communication or communications service within a 'public' communications network, the E-privacy Directive might not be applicable.

A third problem to be mentioned relates to the difference in rationale and scope of Directive 2002/58/EC, leading to the question whether sensor-based systems and chip-card-based payment systems fall within the scope of the definitions of communication networks and services. In our view, on the basis of the rationale behind Directives 2002/21/EC and 2002/58/EC, as well as the recitals and provisions of these Directives, the conclusion should

be that they are not aimed at such systems. The Directives seem to be aimed at intentional communications in which the content of the communication plays an important role. However, an analysis of the definitions of electronic communications networks and services as well as the definition of communication shows that they are very broad in scope, leaving room for application to sensor-based systems and chip-card-based systems.

A final group of problems relate to the obscurities and problems that exist regarding consent as the sole ground for the processing of location data. Not only is it problematic how to give consent (unambiguously? in writing?) and whether it can be given freely (e.g. in the case of a hierarchical relationship), but it is also unclear who should obtain consent from whom. Here, the difference between two- or three-party structures is important, as well as the distinction between user and subscriber to a service.

In a three-party structure, such as Cell-ID, a third party provides a network that generates the location data. The user of a service gives his prior informed consent to the provider of the service. This provider has to receive location data from the network provider. In these situations, consent to use location data in order to provide a value-added service also needs to involve consent to transfer the location data from one provider to the other. However, it is not completely clear within these structures if, and if so who, should obtain consent from users, the persons whose data are in effect being processed by the system. Recital 31 of the E-Privacy Directive does give some insight into this issue, but certainly does not provide a clear answer for each and every situation:

> "Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it."

On the basis of the definition of consent as laid down in the Data Protection Directive, as well as on the basis of the opinion of the Article 29 Working Group, we are of the opinion that in case of a subscriber using a location based service in order to track and trace users, consent needs to be given by both the subscriber as well as the user. This should be made explicit within the legal framework. In this respect it is advisable to also clarify the information duties, in a sense that in case a subscriber is using a service to track and trace other users, the duty to inform the user will be on the subscriber.

9.2.3 Data Retention

Directive 2006/24/EC (hereinafter: Data Retention Directive) regulates the mandatory storage of traffic data. The Directive excludes the content of messages from the obligation of data retention. In view of Location Based Services, particularly the data mentioned in article 5 paragraph 1 under (f) is relevant:

> "data necessary to identify the location of mobile communication equipment:
>
> (1) the location label (Cell ID) at the start of the communication;
>
> (2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained."

Even though this Directive is introduced to harmonise the obligation of data retention, the margin of discretion left to the Member States is too large to achieve this aim. On the basis of article 6, the required duration of storage is at least six months with a maximum of two years.

Another problem is embedded in article 4 which states that data shall only be provided to competent national authorities: "Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law." This does not provide guidance for national law on the conditions under which law enforcement agencies can access location data, however.

9.2.4 Employment relationships

As described in chapter 4, no specific European legislation exists in view of the processing of data within employment relationships. The general rules as laid down in Directives 95/46/EC and 2002/58/EC are applicable within the boundaries of these directives. However, the Article 29 Working Party has already on several occasions drawn attention to the specific problems that arise with regard to the processing of personal data within employment relationships. One of them being the question as to whether consent by employees to surveillance by employers can be freely given.

Other points of interests raised by the Article 29 Working Party relate to the requirement that processing of location data on employees must correspond to a specific need on the part of the company which is connected to its activity; the fact that the purpose of the processing may not be achievable by less intrusive means; the requirement that equipment should offer the possibility to switch the location function of, as employer's should not collect location data relating to an employee outside working hours; the statement that a reasonable retention period should not supersede two months; the requirement that employers should take adequate measures to restrict and secure access to location data; and the issue of properly informing employees about the possibility) to be monitored.

9.3 Implementation of the legal framework within Member States

9.3.1 Introduction

From the country chapters it becomes clear that most of the problems described above also exist within the Member States as a result of implementation laws that resemble the European Legal Framework to a large extent. This holds true not only for the general obligations and rights, but also for the exceptions to the general rules.

Also with regard to the LBS that are provided within the different Member States discussed, it can be concluded that they are very similar in kind. In this respect, mention can be made of services enabling the positioning of a cell-phone in case of an emergency; automatic payment services; traffic and fleet management; direct marketing services; tracking services for children, vehicles and employees; and electronic bracelets for elderly persons and convicted felons. Within Germany and France initiatives of car insurance companies to track and trace their users in order to provide them with an insurance completely suited to their driving habits have encountered concerns from the data protection authority, leading to a prohibition of this system in France.

9.3.2 General legal framework

In all the countries described, the legal framework is implemented within general laws regarding data protection, telecommunications and electronic communications. Some striking issues regarding the implementation will be mentioned in this subsection, without being exhaustive.

In Germany, besides the Data Protection Act and the Telecommunications Act, also the Telemedia Act (TMG) is of importance. This act concerns telemedia services which are defined as all electronic information or communication services which are not telecommunications services. The content of a LBS is regarded a telemedia service as it exceeds common telecommunications services like voice communication, SMS and provides new, multimedia content. The existence of these two separate laws has as a consequence that content providers in Germany have to comply with the provisions set out in the Telemedia Act, and telecommunications providers must comply with the regulations of the Telecommunications Act. The transmission of location data from the telecommunications service provider (TSP) to the content provider (CP) usually is within the scope of the Telecommunications Act, while the use of location data to provide the LBS is covered by the TMG.

In the Netherlands, the provisions regarding traffic data and location data are implemented within the Telecommunications Act and resemble the E-privacy Directive to a large extent, with the exception that article 5 is not implemented. The explanatory memorandum of the Dutch Telecommunications Act stipulates in this respect that further research is needed and that the article will not be implemented so far. However, this does not imply that there is no regulation on the confidentiality of communications in the Netherlands. Article 13 of the Dutch Constitution (Grondwet) provides a general right on confidentiality of communications.

In Belgium, the Electronic Communications Act was introduced in 2005. This Act complements the general rules provided by the Data Protection Act. At this moment, two law proposals are pending to adjust the provisions of the Electronic Communications Act in order to solve the specific issues related to Location Based Services.

In France, all personal data processing should comply with the provisions of the Data Protection Act. However, when location data are originated from a public electronic communications network, supplementary safeguards have been introduced by Article L.34-1 of the Posts and Electronic Communications Code, which transposes Directive 2002/58/EC. French legislation only provides a definition of location data in the context of electronic communications where it means “data allowing the localisation of the user’s terminal equipment”. However, this definition does not specify which kind of data it refers to.

9.3.3 Law enforcement and employment relationships

All the Member States discussed have specific rules within their Criminal Proceedings Act regarding the use of and access to location and traffic data by law enforcement authorities. Even though there are differences with regard to the persons who have the authority to use and access location data, as well as regarding the scope of the provisions, in general it is possible for law enforcement to request and access traffic as well as location data in all the countries discussed.

In general, there are no specific rules for the processing of location and traffic data within private relationships. However, in all the Member States described, the general rules as laid down in the implementation rules do apply to private relationships, such as employment relationships. Moreover, national data protection authorities as well as national courts have given some insights regarding the way in which the processing of (personal) location and traffic data within employment relationships should be dealt with.

In all the Member States, Labour Law provides a specific obligation requiring involvement of the company's works council or the trade union when technical equipment aiming at monitoring employees is being installed. However, consent of the trade union or the works council cannot be a substitute for the individual, free, specific and informed consent of the employee.

In France, Labour Law also contains two provisions in respect of protection of employees' fundamental rights. One concerns the principal of proportionality, the other the principal of transparency. The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*, CNIL) has issued some general guidelines since the year 2002 regarding the cyber-surveillance of workers, defining the rules which should apply to this specific context. In response to the vast development of the location data processing by employers with purposes of improving the production process or of controlling the working hours, the CNIL issued a series of documents, defining the rights and obligations of controllers.

9.3.4 Remaining questions and their national counterparts

As already mentioned, the country chapters show that the questions that remain at the European level regarding the legal framework on the processing of (personal) location and traffic data, also exist to a large extent at the national levels. Due to the obscurities in definitions, the overlap and the scope, it is hard to apply the legal framework in practice, leaving too much room for national legislators, data protection authorities, and national courts to fill in the blanks. Some issues are dealt with at the national level by one of the parties mentioned, while other problems are even worse at the national level because of incorrect or incomplete implementation laws or problematic interpretations of the provisions copied from the directives.

In all the Member States, the data protection and telecommunications authorities provide clarification with regard to the legal framework for the provision of LBS. This is often on the basis of complaints, as mentioned in the report on France, CNIL is receiving each day more complaints and applications for consultations regarding the processing of location data. However, data protection authorities are free to initiate general opinions on their own authority. Again reference can be made to the country chapter on France to illustrate another problem in this respect, namely the non binding character of the opinions of Data Protection Authorities and the uncertainty this leaves from the perspective of legal certainty. For example in France the approval of the Act for the fight against terrorism has shown that the opinion of the CNIL was not always followed and some provisions of the law relative to the systems of surveillance considered harmful by the CNIL, have been validated by the Constitutional Council anyway.

In the Netherlands, it might even be harder to clarify the implemented rules, because two authorities mingle in the discussion regarding the provision of LBS: On the one hand the Data Protection Authority (CBP) and on the other hand the authority supervising the Telecommunications Act (OPTA). From their different perspectives and aims, it could be that conflicting interests would lead to conflicting legal interpretations. Therefore it is of the utmost importance that these protection authorities consult each other.

9.3.5 Some illustrative examples

National interpretations and solutions can not only be problematic at the national level, but can also cause discrepancies between the Member States which can be harmful in view of cross border provision of Location Based Services and cross border protection of fundamental rights such as privacy. In this respect, as an illustration and example, some differences within the described Member States will be shortly mentioned.

In Germany problems can arise regarding consent. As a general rule, the Data Protection Act requires a written consent of the data subject, while the Telecommunications Act lays down a specific provision for consent by electronic means. Consent to use location data that is not anonymized can in Germany only be given by the subscriber. The subscriber shall inform his co-users of all such given consent. This regulation contradicts Art. 6 paragraph 3 and Art. 9 paragraph 1 of Directive 2002/58/EC that require consent of subscribers and users. Reasons given for this derogation of Directive 2002/58/EC are telecommunications service providers' lack of awareness of users other than the subscriber and impossibility to link location data to other individuals than the subscriber whose customer data was collected upon subscription.

In France, Article L.34-1.IV of the Post and Electronic Communication Code can be mentioned. This article acknowledges a specific right to the user of the service, when he is a different person from the subscriber, to suspend the consent given by the subscriber, i.e. to deactivate the localisation device. However, even if the service provider should rely on the previous consent of the subscriber, it is not compelled by the legislation to obtain the previous consent of the user as well.

One of the Belgian Law Proposals tries to solve the issue of who should consent to whom, by obliging the operator of a mobile network to inform, before the subscription to the service, both the subscriber and the user, when they are different persons. It is also intended to compel the operator to obtain the consent of both the subscriber and the user.

Another problem area that remains at the national level relates to the restriction of applicability of the legal framework to public parties and networks of communications. In Germany, the Telecommuncations Act and the Telemedia Act apply only to generating and use of location data by telecommunications service provider and telemedia service providers. If a private party wants to generate or use location data of a third party, a statutory basis is required. As no specific law applies the regulations of the Federal Data Protection Act must be complied with.

In France, the same problem exists as the examples of the use of e-tickets in Public Transport; the taking of automatic pictures of cars when their drivers infringe the Traffic Code; and the use of e-bracelets for offenders show. None of these examples imply the use of a public network of communications and thus Art. L.34.1 of the Code of Posts and Electronic Communications will not be applicable. However, as most of the location data processing by private parties is taking place in the field of public electronic communications networks through the use of Location Based Services. These processing will thus fall under the provisions of both the Code of Posts and Electronic communications and the Data Protection Act.

The lack of clarity concerning certain definitions such as public communications networks and services makes it hard to apply the rules to specific techniques, as it is not always clear whether these techniques are, or are not covered by the legal rules. In the Netherlands several discussions have arisen, for example regarding the question whether RFID and WiFi fall

within the scope of the Telecommunications Act. Because of the absence of subscribers to these systems, it is argued that they do not.

Illustrative in this respect is the opinion of OPTA that considered advertisements transmitted through Bluetooth not to fall within the scope of the definition of spam, because the messages were sent to anyone who passed by, regardless of them being a subscriber to the service or not. However, this might not be the explanation OPTA prefers, as they call on all people who received unsolicited messages to complain.

9.3.6 Data retention

With regard to data retention the different Member States have made a different use of the large margin of appreciation offered by Directive 2006/24/EC. Germany has chosen to introduce the shortest retention period possible and will require six-month retention of traffic data. In Belgium a decree still needs to be issued that will specify the data to be retained; the conditions under which providers will need to register and retain the data; as well as the exact retention period. In the Netherlands a draft Bill to implement Directive 2006/24/EC was published in January 2007. Art. 13.4 of the Telecommunications Act will be extended to require all telecommunication providers to store the traffic data as designated in an Order in Council for a period of 18 months. Not only the location of the cell of origin and the cell of receipt of mobile telecommunications are included, but also the location of any other cell during the communication. The draft Bill has triggered critical reactions not only by the telecommunications industry, but also by the Dutch Data Protection Authority.

In France, three different retention periods, all related to different purposes of retention, are provided for in the Code of the Posts and Electronic Communications. The broad and vague terms used by the legislator compel the Telecommunications Operator to retain a large amount of data, which has been highly criticised by the CNIL.

9.4 In conclusion

The conclusion of this report is that the legal framework for processing location data generated in positioning systems, including LBS, is very complex indeed. With three European Directives that partially overlap, using not mutually exclusive definitions of personal data, traffic data, and location data, it is a Herculean task to determine which legal provisions apply when LBS providers process location data. The Venn diagram in Figure 5 (see section 4.4) showing seven possible combinations of data, often divided in two parts, illustrates this. Likewise, it is not easy to pinpoint the exact conditions under which private parties like employers and public parties like law-enforcement authorities can have access to location data. The picture is compounded by the fact that there exists a wide variety of positioning systems and LBS applications based on diverging technologies, which from a legal point of view cannot be easily categorised under the legal definitions.

Apart from the difficulties arising from the sheer complexity of the legal framework, there are also problems with respect to unclear definitions and unresolved legal questions. Major open questions are whether location data generated by mobile phones in stand-by mode qualify as traffic data, and what is meant by ‘public availability’ of electronic communications networks and services. Also, it is uncertain whether sensor-based systems and chip-card-based payment systems, which can also be used for localisation and monitoring of people, fall inside or outside the scope of the legal framework for electronic communications: the rationale of the directives for these sectors suggests that they are excluded, but the wording of the definitions

allows including them within the scope of the directives. Finally, there are also several open questions with respect to the consent that should in certain cases be obtained for processing location data: who exactly should give consent to whom, and how?

The complexity, unclarities, and open legal questions do not occur only at the European level; they exist similarly in the national legal frameworks we have studied. This indicates that national implementations of the European legal framework have not been able to address the problems that occur at the European level and that are compounded by the development of new location-based serviced and positioning systems.

Another conclusion that can be drawn from this study is that law enforcement authorities have a vast range of possibilities to access and process location data, the scope of which is significantly widened through the recent requirements for traffic data retention, which include location data of mobile phones. Moreover, the lack of specific rules in employment relationships and the lack of applicability of the existing legal framework to private localisation systems, imply that employers have a substantial capacity and authority to monitor the whereabouts of their employees, which are hardly off-set by checks and balances to protect the privacy of employees. As a result, the legal framework for processing location data by public and private parties allows much scope for these parties to infringe the privacy of citizens and employees. With the increasing pervasiveness and accuracy of positioning devices, vast amounts of precise location data are being generated and stored. The fast growth in sophisticated location techniques together with the wide legal scope for processing the resulting location data pose a significant threat to the privacy of European citizens.

Given these conclusions, a first recommendation to be made is that the European legislator investigate whether the European legal framework for positioning systems and LBS can be simplified. Should this turn out to be infeasible in the short term, the European legislator should at least provide more clarity regarding the applicability of the various legal provisions in Directive 2002/58/EC to the various forms of positioning systems and LBS. This clarification should not only cover a schematic overview of which provisions apply to which type of location systems, but also resolve current unclarities and answer open questions. In particular, it should be resolved whether ‘standby’ location data are traffic data, which LBS systems are ‘publicly available’ electronic communications systems, whether sensor-based and chip-card-based systems involve electronic communications, and how consent should be given in the context of location systems.

A second recommendation is that a reassessment of the privacy protection mechanisms in the legal framework for accessing personal location data by public and private parties is warranted. The technical possibilities to generate and store location data imply that the movement of European citizens and employees can be monitored accurately and pervasively, and these possibilities are likely to increase further in the near future. Such pervasive monitoring of citizens’ whereabouts will seriously impact their privacy, and perhaps more checks and balances need to be installed in order to off-set this increasing privacy intrusion.

In conclusion, in view of the fast development of location systems and new communication technologies, a reassessment and clarification of the European legal framework for processing location data is urgently needed, both to adequately protect citizens’ privacy and to foster the development of location-based services in Europe.

10 References

Asscher L. F. 2004. Regulating Spam: Directive 2002/58 and Beyond (May 1, 2004), (available at SSRN: <http://ssrn.com/abstract=607183 or DOI: 10.2139/ssrn.607183>).

Béraldin C. 2007. La mesure de surveillance électronique en Belgique : processus d'institutiionnalisation du dispositif, in Justice et Technologies : Surveillances électronique en Europe, eds. Froment J.-C and Kaluszynski, PUG, 2007, p.117-127.

Beugelsdijk R. 2006. RFID; Veelbelovend of onverantwoord?, CBP oktober 2006.

Boulanger M.-H., Lacoste A-C & Louveaux S. 2003. La surveillance électronique des employés, Revue Ubiquité – Droit des technologies de l'information, n°15/2003.

De Jong J.D.C. 2005. Een juridische blik op WiFi, Wetenschapswinkel Rechten, Universiteit van Utrecht 2005.

ECP.nl 2005. Privacyrechtelijke aspecten van RFID, report mei 2005.

Hallaschka F. & Jandt S. 2006. Standortbezogene Dienste im Unternehmen, Multimedia & Recht, 7/2006, p. 436–441.

Hildebrandt, M. and Meints, M. (2006). D7.7: RFID, Profiling, and AmI, Deliverable. (available at <http://www.fidis.net/fidis-del/period-3-20062007>).

Jandt S. 2007. Datenschutz bei Location Based Services – Voraussetzungen und Grenzen der rechtmäßigen Verwendung von Positionsdaten, Multimedia & Recht, 2/2007, p. 74 – 78.

Grasse D. 2006. Proteccion de los datos personales y geolocalizacion, datospersonales.org, n°21, 3 May 2006.

Hendrickx F. 2005. Privacy and Data Protection in the Workplace: The Netherlands, in: Nouwt S., DeVries B.R. & Prins C. (Eds.), Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, The Hague: TMC Asser Press 2005.

Kölmel B.2002. Location Based Services: Wünsche und Realität, 2002. (available at <http://www.e-lba.com/YellowMap%20LBS%20Wuensche%20und%20Realit%C3%A4t.pdf>).

Kaspersen H.W.K. 2002. Data protection and e-commerce, in: Lodder A.R. & Kaspersen H.W.K. (Eds.), eDirectives: Guide to European Union Law on E-Commerce, The Hague/London/New York: Kluwer Law International 2002, p. 119-145.

Koevoets M.M. 2006. Wangedrag van werknemers; De bevoegdheid van werkgevers tot opsporing en sanctionering, dissertation, Den Haag: Boom Juridische Uitgevers 2006.

Koops B.J. et al. 2005. Aftapbaarheid van Telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet, november 2005.

Mallié C. 2007. La mesure de surveillance électroniques en Belgique, in Justice et Technologies : Surveillances électronique en Europe, eds. Froment J.-C and Kaluszynski, PUG, 2007, p.107-116.

Martucci L. et al. 2006. Trusted Server Model for Privacy-Enhanced Location Based Services. In: Proceedings of the 11th Nordic Workshop on Secure IT Systems 19-20 October 2006, Linköping Sweden, 2006, pp. 13-25.

Moreno O. 2005. La géolocalisation des travailleurs, DroitBelge.net, Actualité, 22 December 2005.

Nassary Zadeh, L. (2007) (forthcoming). D11.2: Location based services (available at <http://www.fidis.net/fidis-del/period-3-20062007>).

Ohlenburg A. 2004. Der neue Telekommunikationsdatenschutz – Eine Darstellung von Teil 7 Abschnitt 2 TKG, Mutimedia und Recht 7/2004, p. 431–440.

Renette S. & De Bot D. 2006. Employee, where are thou? De Belgische wet van 13 juni 2005 betreffende de elektronische communicatie en haar gevolgen voor door een werkgever aangewende geolokalisatiesystemen. Privacy & Informatie 2006/9, p. 210-214.

Rijckaert O. 2005. Surveillance des travailleurs : Nouveaux procédés, multiples contraintes, Droit et nouvelles Technologies, 26 April 2005.

Smits D., Exit-route via GPS?, 23 oktober 2006. (available at: <http://www.expertlog.nl/2006/10/exitroute_via_g.html>).

Terstegge J.H.J. (CBP) 2002. Goed werken in netwerken, Achtergrondstudies en verkenningen 21, Den Haag, april 2002, (available at: <http://www.cbpweb.nl/downloads_av/av21.pdf?refer=true&theme=purple>).

Terstegge J., Zijn uw systemen WBP-proof?, available at: <http://home.planet.nl/~privacy1/wbpproof.htm>.

Tinnefeld M-T., Ehmann E. & Gerling R.W. 2005. Einführung in das Datenschutzrecht, Munich, 2005.

Van der Hof S. et al 2006. Openbaarheid in het Internettijdperk. De invloed van ICT op juridische concepten van openbaarheid, Den Haag: Sdu Uitgevers 2006.

Veldhuijzen A. 2006. Autocomputer is ook bewijs, 20 oktober 2006, (available at: <http://www.ad.nl/autowereld/article730043.ece>).

White J. C., People not places. A policy framework for Analyzing Location Privacy Issues, (available at: <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf>).

WODC 2005. Geboeid door de enkelband, Evaluatie pilot Elektronische Detentie, Nijmegen: ITS, 2005.

Working Party 29 2001. Opinion 8/2001 on the processing of personal data in the employment context, WP 48.

Working Party 29 2005. Opinion on the use of location data with a view to providing value-added services, 2130/95/EN, WP 115, November 2005.

Working Party 29 2006. Work Programme 2006-2007, document nr. 00744/06/EN, WP 120.

Working Party 29 2006. Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive. Adopted on 26th September 2006, 1611/06/EN WP 126.

11 Abbreviations & Glossary

Abbreviations

ATM	Automated Teller Machine
BfDI	*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (German Federal Data Protection Commissioner)
CBP	*College Bescherming Persoonsgegevens* (Dutch Data Protection Authority)
CCC	Council of Europe Convention on Cybercrime
CCTV	Closed-Circuit Television
CDMA	Code Division Multiple Access
CNIL	*Commission Nationale de l'Informatique et des Libertés* (French Data Protection Authority)
DCCP	Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*)
DTA	Dutch Telecommunications Act (*Telecommunicatiewet*)
ECHR	European Convention on Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
GPS	Global Positioning System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications (originally from *Groupe Spécial Mobile*)
IBBT	Intitute for Broadband Technology (Flanders)
ICAO	International Civil Aviation Organization
ISMS	Information Security Management System
IT	Information Technology
JO	*Journal Officiel* (French Official Journal)
LBS	Location Based Service
MM	Manufacturing Management
MO	Mobile Operator
MRTD	Machine Readable Travel Document
OECD	Organisation for Economic Co-operation and Development
OPTA	*Onafhankelijke Post en Telecommunicatie Autoriteit* (Dutch Independent Mail and Telecommunications Authority)
PDA	Personal Digital Assistant
PDPA	Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*)
RFID	Radio Frequency Identification
SCM	Supply Chain Management
SMS	Short Message Service
TKG	*Telekommunikationsgesetz* (German Telecommunications Act)
TMG	*Telemediengesetz* (German Telemedia Act)
UMTS	Universal Mobile Telecommunications System
WAP	Wireless Application Protocol
WiFi	Wireless Fidelity

Glossary

A-GPS	Assisted GPS: Based on GPS, this technology uses an assistance server to cut down the time needed to determine a location.
Bluetooth	An industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices such as mobile phones, laptops, PCs, printers, digital cameras, and video game consoles over a secure, globally unlicensed short-range radio frequency.(source: Wikipedia)

Cell-ID	An identification code sent by GSM masts when transmitting to a mobile device. Each mast has it's own ID.
E-OTD	Enhanced Observed Time Difference: Measures the time of arrival of a base station signal on the handset.
IMSI-Catcher	A device for intercepting the IMSI number of GSM mobile phones.
IP-address	Internet Protocol address. Unique number for each personal computer, comparable with a telephone number.
ISMS	(Information Security Management System) Management system used to ensure the appropriateness, security and adequate use of information.
push service	A service that is triggered on demand of the user. The term originated from the domain of marketing.
pull service	A service that is provided automatically without user interaction. The term originated from the domain of marketing.
traffic data	Electronic-communications traffic data, i.e., data about who telecommunicated with whom when, how long, and where.