FIDIS

Future of Identity in the Information Society

Title:	"D11.2: Mobility and LBS"
Author:	WP11
Editors:	André Deuker (JWG, Germany)
Reviewers:	Patrick McKelvy (SIRRIX, Germany)
	Kai Rannenberg (JWG, Germany)
Identifier:	D11.2
Type:	[Deliverable]
Version:	1.0
Date:	Thursday, 03 July 2008
Status:	[Final]
Class:	[Public]
File:	fidis-wp11-del11_2_Mobility_and_LBS_v1.0.doc

Summary

Mobility and Location-Based Services play an ever-increasing role in everyday life. The spectrum of applications covers services for entertainment purposes as well as services that aim to increase the efficiency of business processes or help in case of emergency. In this deliverable, the impact of Location-Based Services on the identity of an individual is explained. Typical application areas and their impact on user identity are illustrated by exemplary use cases. From a technical perspective the deliverable focuses on various positioning methods as they constitute a prerequisite for the existence of LBS. Furthermore, legal aspects of Location-Based Services are discussed within an analysis of the regulations of the European data protection 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 (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	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 (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	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 (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	02/2004	• Initial release
0.2	10/2007	• New conception of the deliverable after the FIDIS Research Meeting 2008
0.3	12/2007	• Added contributions by ICPP and KUL (ICRI)
0.5	03/2008	• Revised structure including comments of the WP11 Work Shop
0.5	04/2008	• Finalisation of Chapter 5.1 and 5.2
0.6	05/2008	• Finalisation of Chapter 5
0.7	06/2008	• Finalisation of Chapter 4
0.8	06/2008	• Finalisation of Chapter 7
0.9	30.06.2008	• Executive Summary • Version ready for Review
1.0	02.07.2008	• Final delivery version, incorporating the review comments

Contributing Partners:

1. ***JWG:*** Goethe University Frankfurt (Germany)
2. ***ICPP:*** Unabhängiges Landeszentrum für Datenschutz (Germany)
3. ***K.U. Leuven:*** Katholieke Universiteit Leuven / ICRI (Belgium)

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*
1. Executive Summary	André Deuker (JWG)
2. Introduction	André Deuker (JWG)
3. LBS Use Cases	Dr. Martin Meints (ICPP) Christian Krause (ICPP)
4. LBS, Mobile Identities, Profiles and User Control	André Deuker (JWG)
5. Technical Aspects / Positioning Methods	André Deuker (JWG) Denis Royer (JWG)
6. Legal aspects	Eleni Kosta (KUL ICRI)
7. Implications / Relevance for FIDIS	André Deuker (JWG)
8. Bibliography	All

Table of Contents

1 Executive Summary

1.1 Scope

This document is primarily aimed at an audience of academics, EU policy-makers, experts in the fields of technology, law, sociology, and interested citizens. Extending the discussions and findings in FIDIS Work Package 11 on mobility and identity (FIDIS deliverables *D11.1*, *D11.3*, and *D11.5)*, this deliverable focuses on the economic aspects of mobility and identity.

1.2 Structure and Content

Some years ago, the ability of user tracking and tracing was a privilege of governments and extremely determined and resourceful private parties, but nowadays mobility and LBS play an increasing role in everybody's life. The technologies that are described in Chapter 5.1 (network-internal positioning methods) are a result of the technological developments necessary to enable mobile communication services. Especially the cell architecture of the communication networks allows to identify and to localise single users. Thus, the ability of network-internal positioning is in the hands of a few market players per country.

Tracking and tracing using network-internal technologies can be understood as a by-product of providing mobile telephony and data services. But network external positioning methods also gain additional attention. Mobile devices are increasingly featured with modules that allow the use of network-external information sources like GPS, Bluetooth or W-LAN to determine their position.

Following up on the new technological opportunities, new economies and products appear on the horizon: New entertainment services like mobile friend finders (cf. Chapter 3.2) or mobile social communities provide new dimensions of human interaction. But LBS also influence the efficiency of classical value chains and the identity of their employees as it is shown e.g. in Scenario 3: Tracking in the Working Context (cf. Chapter 3.3). Chapter 4 has shown that LBS can have major impact on the mobile identities and that the control of the mobile identities can depend on the properties of the LBS.

Tracking and tracing is becoming more and more a commercial product. The providers of such services are obliged to fulfil the legal requirements with regard to the users' privacy. Although many data protection aspects are covered by the European data protection laws the technical evolution comes along with an evolution of possible privacy threats (cf. Chapter 6), especially since the legislator can react solely to foreseen or already present situations. The responsibility for the users' privacy and the protection of their identity thus rests also in the hand of the providers of LBS. A shift of responsibilities between public and private players with regard to data protection and identity management duties is possible. In this situation, the ability of users' to control their privacy and identity is a major aspect.

The development of the new markets and products give reason to further observe the legal, the technological and the market situation that determine the further / future impact of LBS on users' mobile identities.

2 Introduction

Mobility and Location Based Services (LBS) play an increasing role in everybody's life. Their spectrum of application covers services for entertainment purposes as well as services that aim at increasing the efficiency of business processes or help in case of emergency.

Consequently LBS have a major impact on the identity of a person as described and explained in **Chapter 3**, that gives an overview of the different LBS application areas by describing three exemplary use cases and their implications. Then in **Chapter 4** the context awareness of mobile services and especially of LBS and their consequences for users' mobile identities is discussed.

Following up on the new technological opportunities, new economies and products appear on the horizon. Tracking and tracing is becoming more and more a commercial product. This development is based on a technical evolvement of positioning technologies and their diffusion. Mobile devices are increasingly featured with software and hardware modules that enable them to use decentralized technologies like GPS, Bluetooth or W-LAN to determine their position. Also the development of more centralized network based positioning methods progresses. **Chapter 5** gives an overview about the different positioning methods and puts a focus on the precision of the obtained positioning information.

Obviously the enhanced positioning precision holds also risks, e.g. for the privacy of citizens and users. Therefore in **Chapter 6** the European Data Protection Framework is observed with a special focus on the LBS relevant legal aspects. The deliverable concludes in **Chapter 7** with a summary and an outlook.

3 LBS Use Cases

In this chapter, the impact of Location-Based Services (LBS) on the identity of a person is described and analysed. To this regard, the model of partial identities, widely used in the research of FIDIS, is applied. To do so, three scenarios in the context of private life and mobile work are used.

3.1 Introduction

LBS can be considered more complex compared to "*classic*" mobile communicational relationships. This is due to the increased number of workflows and thus communication partners being involved. Depending on how data is collected, processed, stored, and used, there may be different impacts on identity. Again, the influence or control over workflows and policies is a critical factor for the impact of these services on identity, as initially described in D11.1[4]

Location and service data can (potentially) be used, by applying profiling methods, such as those that are used for marketing purposes. In these cases, the user of such services may receive additional partial identities, which are derived from the data his profile is built of.

In this chapter we will use the understanding of partial identities described in FIDIS deliverable D2.1[5] and D11.1.

In general, the relations between the communicating parties relate to the number and the roles of parties and the used workflows. In LBS use cases, they are usually more complex, than in the initial mobile use cases, that had been analysed in D11.1, chapter 3 (Royer, 2005). Therefore there are at least four potential roles to discriminate:

- ***Data subject*** (This is the user of the mobile phone that is located) or ***data object*** (location of for example a vehicle, container or a point of interest such as a restaurant). In some cases a data object that is tracked by an LBS is linked to a specific person
- ***Mobile communication provider*** (provides – as far as no network-external location service such as GPS is used – the location data concerning the mobile phone requesting an LBS to the Location Based Service provider.)
- ***LBS provider*** (provides the additional service using the location data of the data subject or object and matches them with a geo database)
- ***LBS user*** (uses the LBS)

When analysing the influence of LBS on identity we naturally are interested in data subjects, not data objects. Location data typically is not acquired for subjects directly, but for specific objects such as a mobile phone or a special tracking device for example composed of a GPS locator and a communication device. In these cases the link between the object that is located and a corresponding subject is of high interest. Most LBS such as friend finders or kid tracking services base on the assumption, that a device is linked to exactly one person and that this link is very robust, e.g. that the device usually stays with the person.

---

[4] Royer, Denis (ed.): '11.1: Collection of Topics and Clusters of Mobility and identity – Towards a Taxonomy of Mobility and Identity, FIDIS deliverable WP11, 2006.

[5] Nabeth, Thierry; Hildebrandt, Mireille (eds.): '2.1: Inventory of topics and clusters, FIDIS deliverable WP2, 2005.

LBS Usage scenarios show a big variety. This also holds for the roles involved. In many cases some of the four roles introduced above can be taken by one person or organisation simultaneously. An example for this is the use of mobile navigation, where data subject and LBS user can be the same entity.

With regard to the activity and initiative of the parties, typically two types of LBS are used:

- ***Pull services:*** in this case each transaction of the location based service is initiated by the user and the corresponding service data is returned to him.
- ***Push services:*** in this case the transactions of the location based service concerning a data subject or a user are initiated by a third party (maybe after the data subject or user had initially ordered the service).

As described in D11.1, three factors are having the highest influence on partial identities:

- Data including an identifier (especially in its function as address for communication)
- The workflows or processes, in which identity data and the identifier can be used
- The context-dependent policy on how to use the identifier in which workflows or processes

3.2 The Use Cases

Due to complexity of the communicational relationships and the number of different LBS offered on the market, the number of possible scenarios is manifold. Therefore three scenarios were chosen to show the various impacts with regard to the identity of a person. These are especially scenarios with a data subject or with a data object that is closely and directly linked to a data subject. The three scenarios selected are:

- Scenario 1: Using LBS within the private communicational context in cases of emergency (emergency calls and emergency location)
- Scenario 2: Using a friend around service within the private communicational context
- Scenario 3: Using LBS for tracking in the communicational working context

3.2.1 Scenario 1: Location in case of a medical emergency

In this scenario, Alice uses a mobile phone together with a special medical emergency service. In case she uses the emergency button on the phone, her GPS location data is automatically transferred together with her call to a specific rescue control centre. The rescue control centre is able to send medical professionals (if needed with special equipment, e.g. if Alice's location is somewhere in the high mountains) to the location where Alice submitted the emergency call (pull service). Except for emergency calls, her location data is not collected, nor transferred or stored by the service provider.[6]

In this scenario, data processed and stored in emergency cases are being deleted by the service provider after the end of one accounting period of the medical professionals and rescue services involved (in general one year). So her location data is (in general) not available for profiling purposes. In the chosen scenario, the rescue control centre performs its service in the

[6] A service as described is offered for example by the Vitaphone GmbH: http://www.vitaphone.de/de/

European Union. Accordingly, it complies with data protection legislation, such as European Directive 95/46/EC, and implements a high level of IT security related technologies.

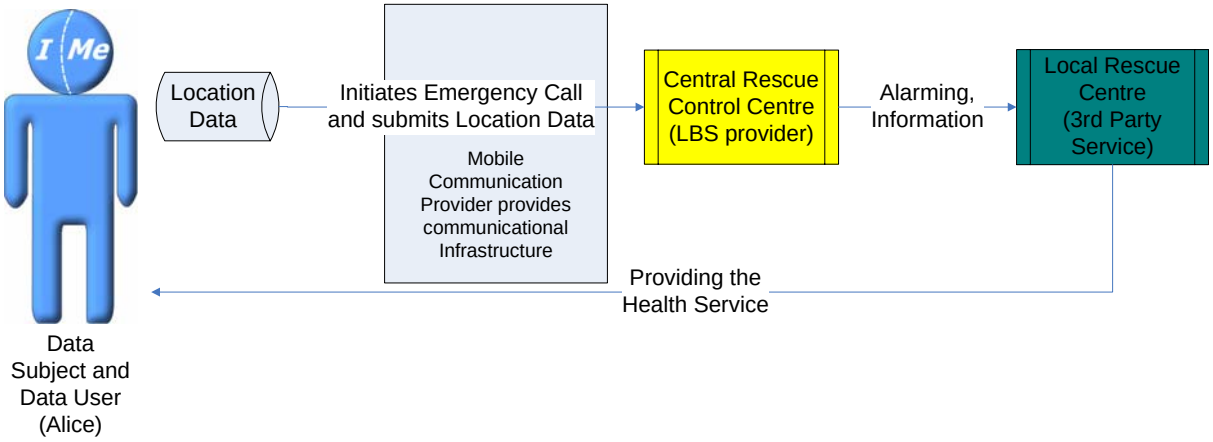

Figure 1: Workflow in the medical emergency scenario.

At the same time, Alice is data subject and user, as she transfers her own location data in a special situation for a special purpose to a special service provider (in this case the rescue control centre). The workflow to be used in cases of emergency is strictly defined and agreed by all participants in the communication, the communicational policies of Alice and the LBS provider match in this example. This communicational context, which is more complex compared to the examples discussed in D11.1, raises questions of data protection and multilateral security, as not all of the personal data remains under Alice's control. In this example, the rescue control centre is aware of these issues and takes care of them by applying appropriate measures for data protection and IT security. The use of LBS in cases of emergency has no significant impact on the identity of Alice when carried out in the described way.

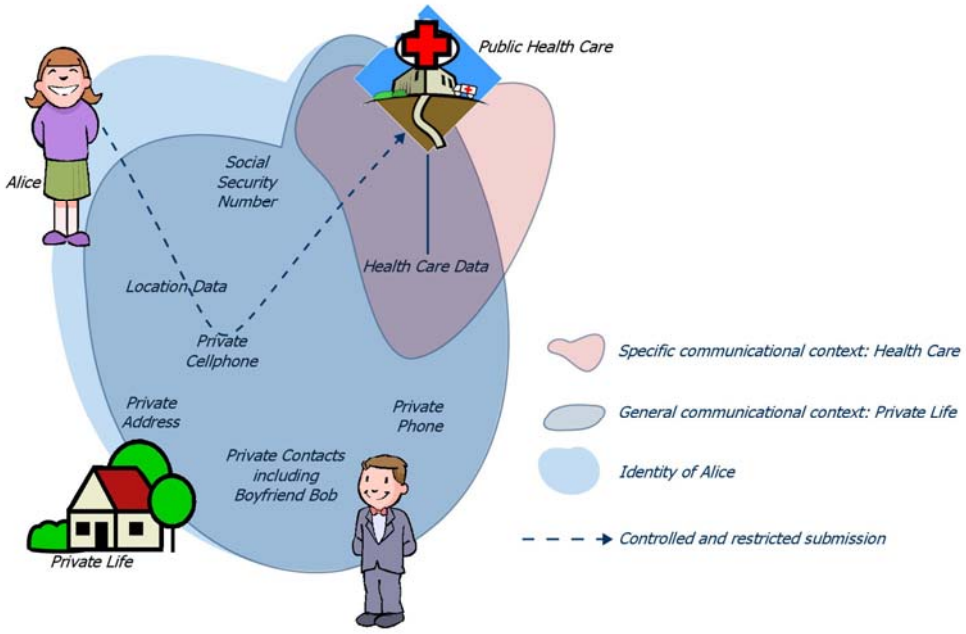

Figure 2: Identity of Alice in the medical emergency scenario.

3.2.2 Scenario 2: Using a friend finder service

In this scenario Alice uses a so-called *friend finder* or "*buddy alert*" service. All persons for which the use of the location service is possible, need to be client of the same service provider. In addition, they have to edit service preferences, allowing each other to exchange location information. Using location data from various telecommunication providers, the (pull) service informs a requesting user via SMS, how far away a certain person is from the user's current location. In return, the person whose location was inquired gets a message informing it about the distance to the requester (push service). If both are close enough and interested, they can get into contact via mobile phone to arrange a meeting.

Alice is registered for this service. Via SMS or web front end she administers a list with her friends on a central server of the LBS provider. Her boyfriend Bob is on that list as well. Bob in turn is client of the LBS provider and has Alice in his list of friends as well. So the location service can be used by both.[7]

[7] An Example for such a service is offered by the Mobiloco GmbH: http://www.mobiloco.de/html/index.jsp

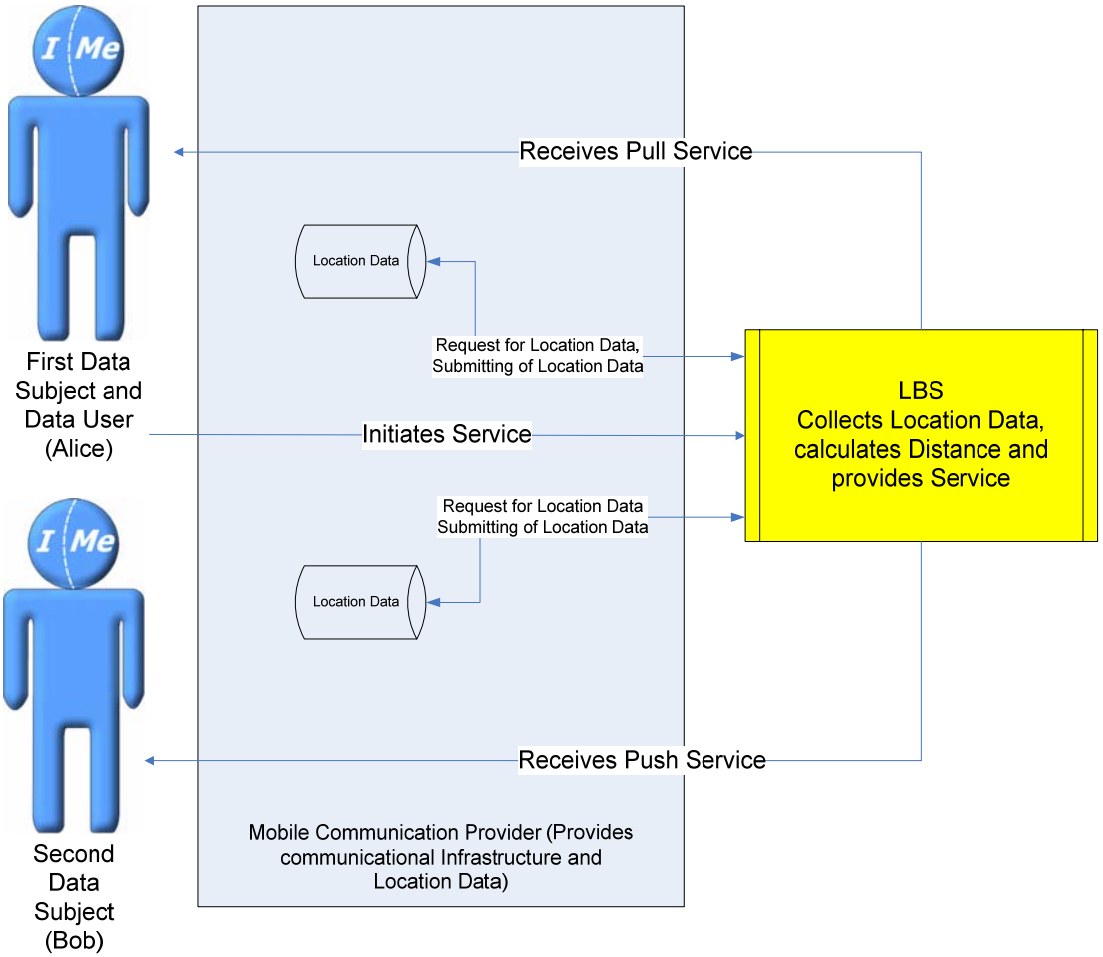

Figure 3: Workflow in the friends around scenario.

In this scenario workflows and the communicational policy are predefined by the LBS provider. The users (data user and data subjects) accept and agreed by signing the contract and by editing a profile (as described above). In this example there is a general consent among the users to use the service. The person whose location is requested is subject of a push service and has no opportunity to declare an individual consent. In any case, location data is generated and processed.

In order to protect the private sphere of the user, the location data in this scenario is blurred. This is done by not transmitting the exact location of the users but only transmitting information on the distance between the users. This blurring of precise location data is part of the communicational and privacy policy of the LBS provider.

There is no need to store any detailed or blurred location data for accounting purposes after they are submitted to the users. In this scenario, the LBS provider does not do so, as laid out in his data protection policy. Therefore, he follows the data minimisation principle stated in the European Directive 95/46/EC. Therefore location data generated by this service cannot be easily used for profiling purposes.

Compared to the Scenario 1, the impact on the identity of the users of the LBS can be more severe, especially in cases where somebody else is initiating the service. For example when

Bob has scheduled a business trip to the capital and on that date and time the service locates him at a nearby beach resort, this reduction of his private sphere can have major impact. As this service can be initiated by all members of a group of trust (in this case Alice and Bob), this reduction of the private sphere can happen to all of them, as their control over the workflow is limited. A process asking for individual consent before any tracing transaction would be more privacy respecting, but probably not practical. In addition this service can cause severe problems when the link between a user and "his" tracked device is not robust.

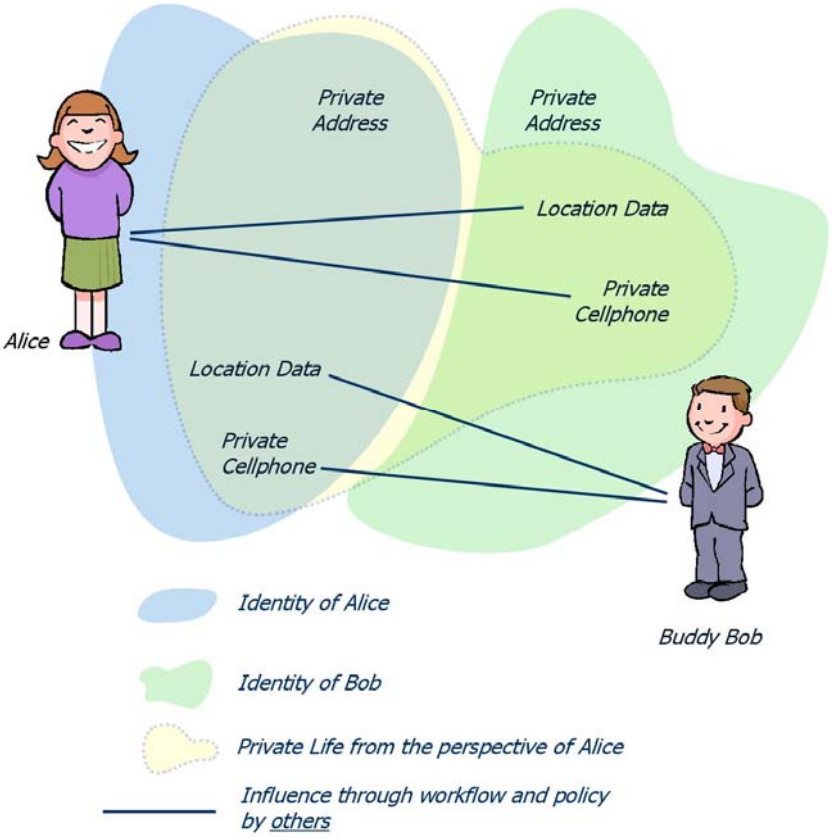

Figure 4: Identity of Alice in the friend around scenario.

3.2.3 Scenario 3: Tracking in the working context

In this scenario, a mobile phone with GPS locator is installed in a transportation vehicle (e.g. a lorry) to track it on its way to different destinations in Europe. Alice is the driver of that lorry and thus has highly flexible working hours. From a central server, the mobile phone is called regularly to submit the current location of the vehicle (pull service from the perspective of the data user, Alice's employer). The submitted location data are stored in a central database.[8] This data is used to track and trace the lorry. In case of significant discrepancies,

[8] A number of technical solutions for this purpose are available on the market for example provided by the Siemens AG (http://www.innovations-report.de/html/berichte/verkehr_logistik/bericht-31185.html) or Ergon (reference implementation under http://www.ergon.ch/doc/Referenz_btl_de.pdf)

compared to the route plan, the employer calls Alice, asks for the reason and discusses with her modifications of the route plan. The location data and additional information from Alice, such as data concerning the traffic situation, is used for further planning of the routing. (In addition the location information is used to monitor Alice in her function as driver of the lorry – at least in a general sense.)

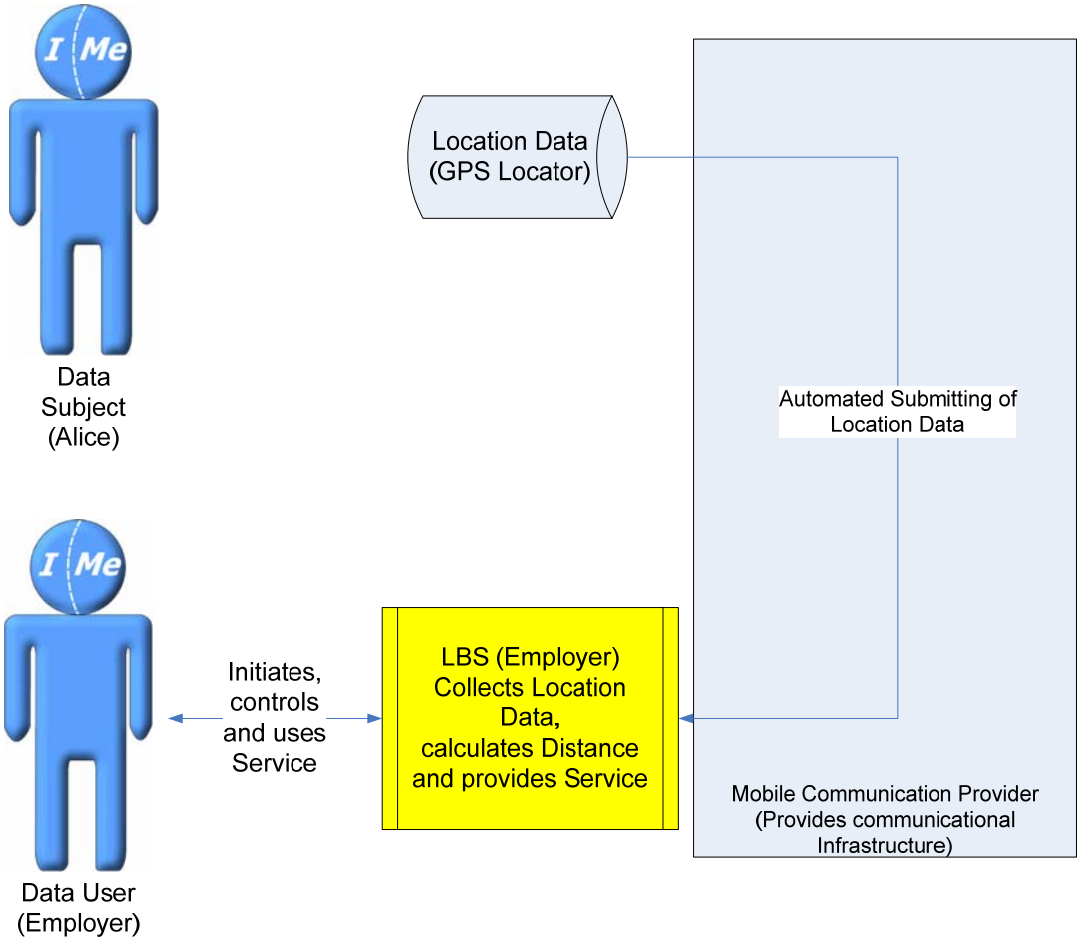

Figure 5: Workflow in the lorry tracking scenario.

In this scenario, the employer of Alice is LBS provider and user, while Alice is a linked data subject. She is subject to workflows and communicational policies defined by her employer. In difference to scenarios 2 and 3 discussed in chapter 3 of FIDIS deliverable D11.1, her location data is generated, stored and analysed by her employer. Consequently, he or she has complete control over her location data, which is monitored by this service.

This kind of profiling leads to a reduced private sphere (at least when working and being on business trips) and reduces her autonomy and flexibility when doing her job. In addition Alice's location data may be attractive for third parties and thus has to be subject to the application of strict data protection rules and a high level of IT security. The application of data protection and IT security clearly is the responsibility of Alice's employer.

In this example the location data of Alice is being used to supervise her while she is doing her job. In such situation consent for processing and storage of her location data cannot easily be base on a free will as required by the European Directive 95/46/EC. In any case, transparency concerning used personal data, the way of processing, and the use of the results by the employer has to be documented and agreed on – for example as part of the employment contract.

In some European countries this is also subject to approval by a workers' council, which is (for example in Germany) stated and regulated by a Works Council Constitution Act.

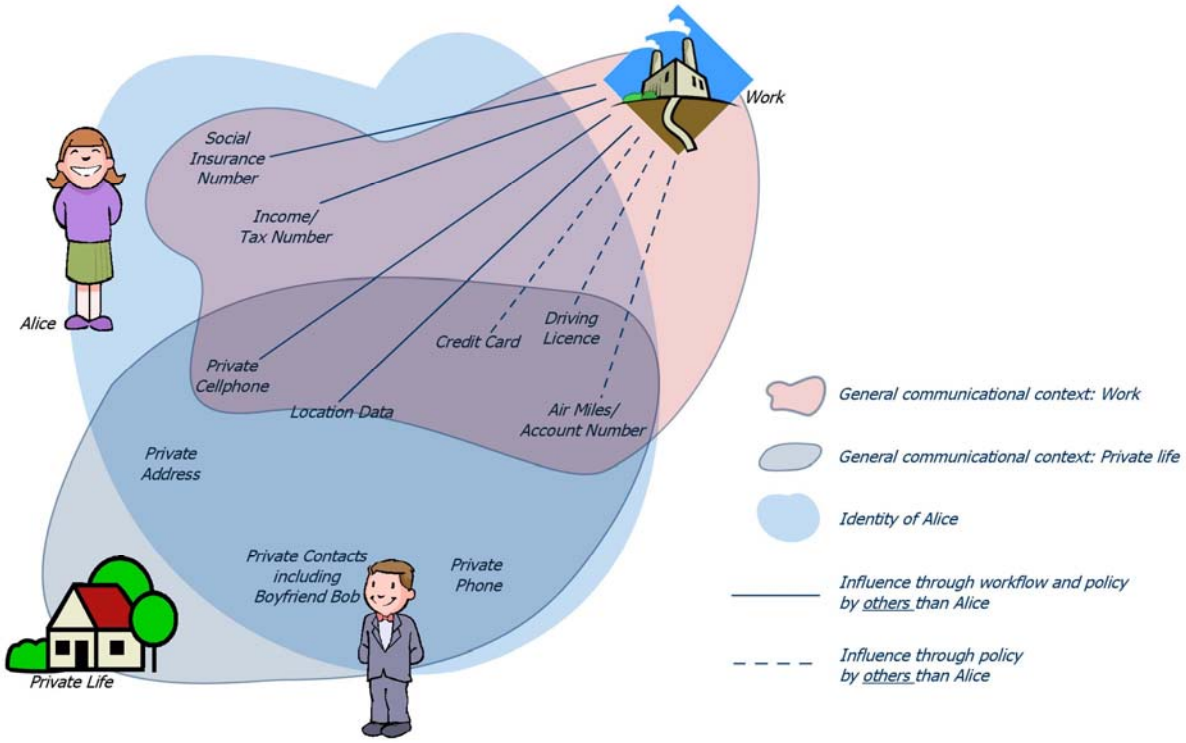

Figure 6: Identity of Alice in the mobile working scenario.

4 LBS, Mobile Identities, Profiles and Users' Control

Referring to FIDIS deliverable D11.1, mobile identities can be described as:

> *"[…] a partial identity, which is connected to the mobility of the subject itself, including location data. The mobile identity may be addressable by the mobile ID. (…) Furthermore the mobility of a subject may be observed by others including the deployment of tracking mechanisms with respect to biometric properties, e.g., by a comprehensive video surveillance."*(Müller et al., 2005)[9]

Looking at the properties of mobile services in general, especially the context awareness of mobile services can affect the impact on a user's mobile identity, when using a LBS.[10] The availability of user's location combined with information about the interests or combined with information about the area he / she is situated in lead to a better understanding of the present user context. Mobile services allow to consider the following types of user contexts:

- **Local context**
  (user's current place / time)
- **Action context**
  (user's current place / time combined with geo data)
- **Time context**
  (user's current time combined with time relevant information)
- **Interests specific context**
  (local, action and time context combined with personal user preferences)

Assuming that the different types of available context information affect a user's identity, the mobile identity consists of the user's time, location and attributes that have been derived from combining location and time information with relevant information about the user's self (e.g. interest specific context) or about the location of the user (action specific context).

Figure 7 shows how LBS can extend Alice's mobile identity through connecting her local context with additional geo information about the area she is situated in. In this example, Alice is at a certain time (Saturday, 3 p.m.) at a certain place (soccer stadium).

The external geo context information is a soccer match that takes place in the stadium at this point of time. A possible assumption and extension of Alice's mobile identity could be that Alice is currently watching soccer. Any person or service that has this background information about Alice's location can attribute this (subjective) action specific context to her identity creating a profile of Alice.

[9] Royer, Denis (ed.): '11.1: Collection of Topics and Clusters of Mobility and identity – Towards a Taxonomy of Mibility and Identity, FIDIS deliverable WP11, 2006, S. 31

[10] [ReicMeieFrem2002] Reichwald; Meier; Fremuth: Die Mobile Ökonomie – Definition und Spezifika, in: Mobile Kommunikation, Gabler, Wiesbaden 2002, 4-15.

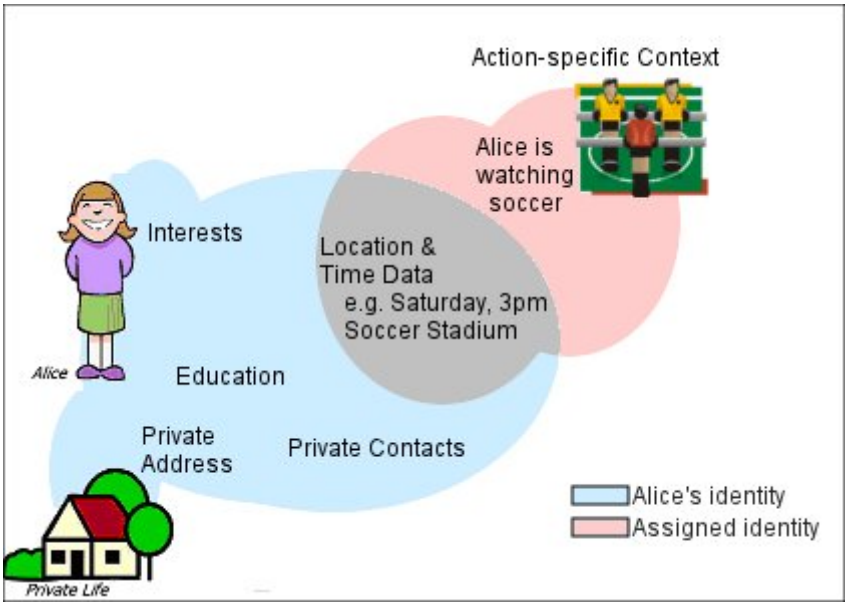

Figure 7: Extension of the Mobile Identity through the Action Specific User Context.

To a certain degree, the (profiling) conclusions that can be drawn about Alice's identity by using her action specific context are out of Alice's control. Thus, the amount of control users have about their identity can depend on the type of the location based service.

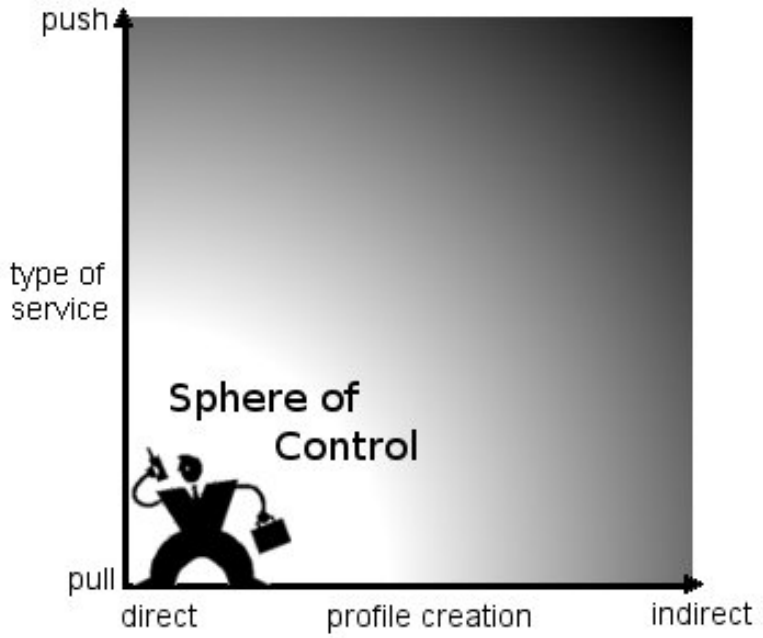

Figure 8: Impact on users' control depending on service properties.

The perceived control with regard to the mobile identity depends on two factors:

1. On the way the service is initiated (push vs. pull) and
2. On the way the profile is created (direct vs. indirect)

A high control is possible if the data subjects / users are able to initialise the service by themselves (pull service). In this case they are aware that the service is enabled and can estimate the types of data that will be processed in order to provide the service.

Another aspect that affects the users' control about their mobile identity is the way how their user profile is derived. The user profile can be a critical piece of information as it is the baseline for the derivation of the interest specific context. Control of the user profile thereby influences the amount of users' control about their mobile identity. Direct profile creation means that the user himself is able to deliver and change the data of his user profile (maybe supported by an identity management system). Indirect profile creation is done by a third party. The data subjects / users even may not be aware that such a profile is created. If the information of the user profiles does not match with the real identity profile, the wrong conclusions can be drawn and assigned to one's identity. In any case it clear, that LBS have a major impact on the (mobile) identities of persons.

5 Technical Aspects and Positioning Methods

A common LBS architecture consists of three parties: The *Mobile Operator*, the *LBS Provider* and the *Mobile User* (cf. Figure 9). Usually, the Mobile Operator works as intermediary between the actual provider of the service and the user. This includes the identification of the customer for payment purposes, the transmission of user's location to the LBS Provider and the transmission of the service itself via mobile communication networks. The LBS Provider combines user's location with relevant geo information in the process of creating and delivering the requested service. Thereby, the action-specific user context can be derived. This deliverable will focus on the presented classical architecture. However, further architectures exist as e.g. the architecture of usage scenario 3 – tracking in the working context (chapter 2.4.3).

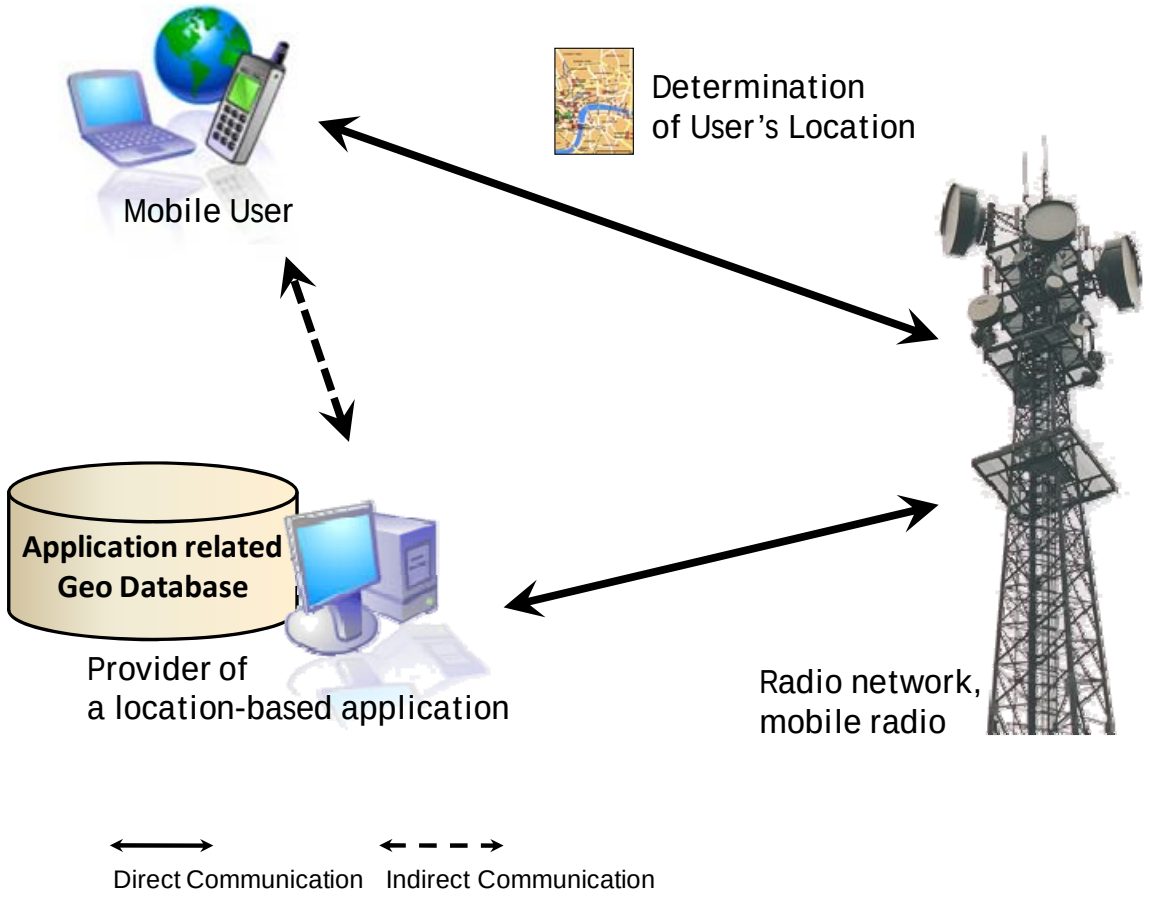

Figure 9: Example for a location based service (LBS) infrastructure and the involved parties.[11]

The availability of user's current location information is the precondition for the existence of LBS. The degree of precision that is obtained by the different positioning methods directly affects user's idem identity as it is a more or less concrete observable attribute of his identity (cf. Chapter 5.3 for details). The way how user's identity is determined affects the level of

[11] Assumption: LBS user is directly connected to the data subject.

control he has about his idem identity. Thereby a smaller level of control about this attribute of his identity can also affect his idem identity.

In the following sections, we make a distinction between network-external sources of location and network-internal sources of location. A user can be located and tracked by using network-internal positioning methods (e.g. by cell of origin positioning). This can take place even without them noticing. In contrast, they have a certain amount of control with network-external positioning technologies.

5.1 Network-external source of location-information

Network-external means that the positioning system is outside the control of the Network Operator and provided by a third party / third system. Common external sources of positioning information are user input, satellite based positioning systems, such as the widely used Global Positioning System (GPS) or the newly emerging Galileo positioning system, position senders, such as radio or infrared beacons, Wireless LAN positioning and peer-to-peer positioning.

5.1.1 "User" as source of positioning information

Having the user as source of location information for the provision of location based services is a "*double-edged sword*". One of the key advantages is that the user keeps the positioning process under his control. That means that he can decide whether he wants to provide positioning-information, when he wants to provide positioning information (so there is no automatic tracking possible) and what kind information concerning the degree of precision of the positioning information he wants to provide to the LBS-provider. The degree of precision can vary from general information (country, city) to more concrete information like e.g. ZIP-code or address. Additionally, the provision of positioning information via the user is possible using almost every kind of terminal or medium.

In contrast to automatically derived and processed positioning information, the "manual" way to provide the current position is much more inconvenient and time consuming. Additionally, the user can only provide positioning information if he is able to localise himself in the area (familiarity with the location). That might be no problem for more general location information like country or area, but it gets gradually difficult with a rising degree of required precision for the provision of location information. The most precise way to locate someone may be to provide an address. However, this is only possible in more densely populated areas.

5.1.2 Satellite based positioning information

Theoretically, the determination of someone's position using satellites can be carried out all over the world.[12] Satellite based positioning is characterised by a unilateral way of communication, as the mobile device only passively receives location information. The accuracy of satellite based positioning is between 1 and 15 meters depending on the used service / technology (c.f. Chapter 5.3).

[12] Cf. Schiller 2004 S. 181

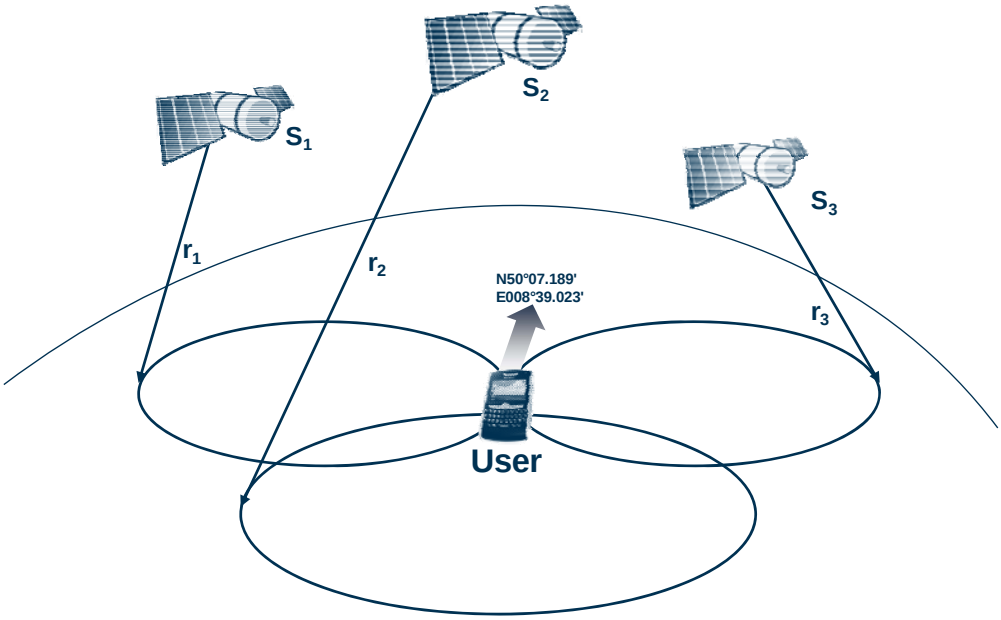

Figure 10: Satellite based location tracking needs at least 3 satellites to triangulate the position of a device or person.[13]

The position of the user can be determined by using the position signals of at least 3 satellites that move on fixed orbits (cf. Figure 11).[14] Satellite based positioning systems have the following (dis-)advantages:

- **(+)** High availability
- **(+)** High precision
- **(+)** Relatively low cost for chipsets that can be embedded in terminals.
- **(-)** High time needed for the initialization of the positioning process
- **(-)** High-power consumption especially in the non-stop-positioning mode.
- **(-)** Signal strength: It is mostly used outside as the signals are generally too weak to be received inside buildings.

The world-wide standard for satellite based positioning still is the Global Positioning System (GPS), established and controlled by the USA. The accuracy of the GPS can be altered in case of military emergency. The forthcoming European satellite positioning system Galileo is planned to be implemented by 2011-12[15] and should obtain a higher accuracy than GPS.

[13] Cf. Schiller 2004 p. 181
[14] Cf. Schiller 2004 p. 182
[15] www.esa.int/esaCP/SEM8LNN0LYE_Benefits_0.html

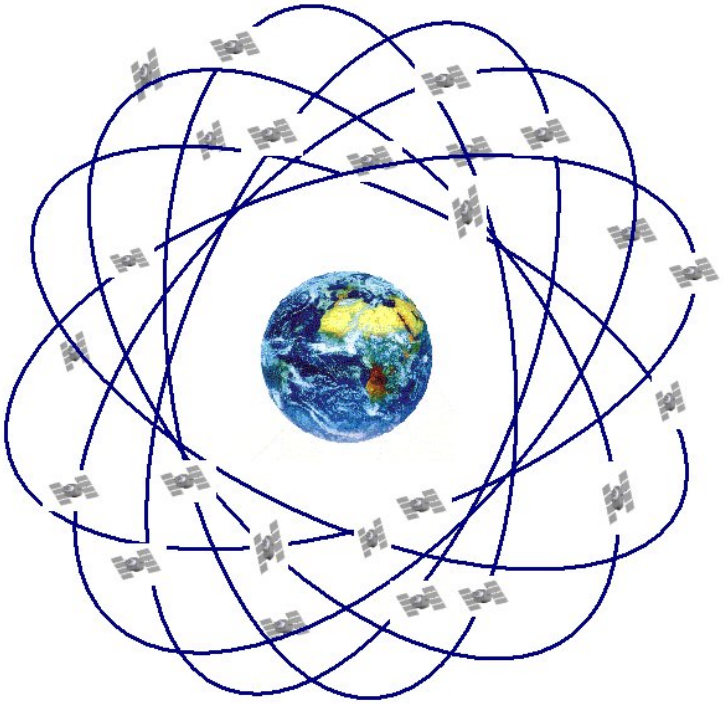

Figure 11: Positioning satellites orbiting the earth.[16]

5.1.3 Further external information sources

Another method to allow positioning is the usage of position transmitters that communicate their location to a user's device via e.g. radio or infrared signals submitted by a beacon within a given area (cf. D11.5 and D7.7 for example applications). The accuracy of the location information thereby depends on the size of this area and can vary from 10 centimetres to several meters. Common usage scenarios for position transmitters are exhibition information systems, museum guides, tourist guides or promotion activities.

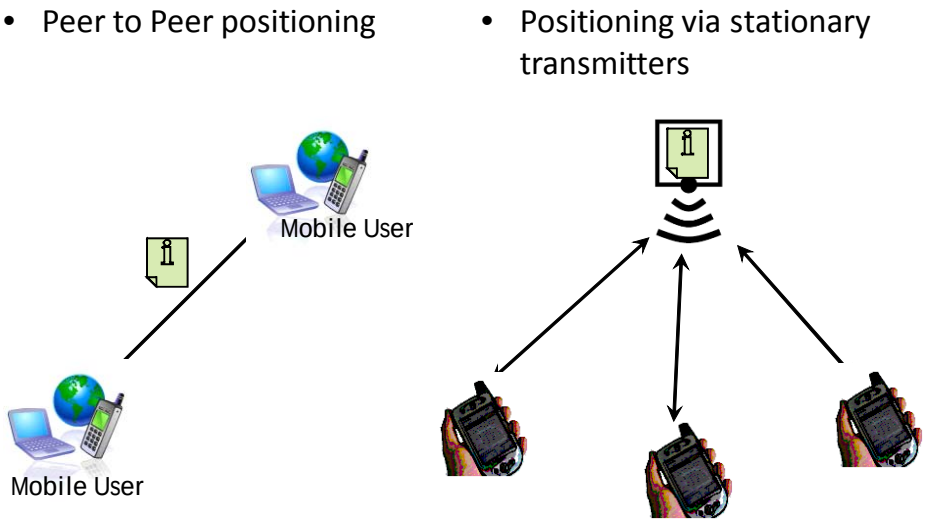

Figure 12: Peer to peer versus stationary transmitter positioning (e.g. by radio or infrared beacons).

[16] Cf. www.fc.up.pt/lic_eg/imagens/gps-const.jpg

W-LAN Access Points (esp. relevant in urban areas), peer-to-peer positioning or Radio Frequency Identification (RFID) are further relevant technologies / methods to determine users' location.

5.2 Network based source of location-information

Network based positioning is based on the fact, that the user of location based services on mobile phones is connected to the mobile communication network (e.g. GSM or UMTS based mobile networks). The network itself is constructed of many (overlapping) network-cells, whose shape is influenced by the environment (buildings, etc) and usually neither hexagonal nor a perfect circle, even though this is the usual way of drawing them (cf. Figure 13).

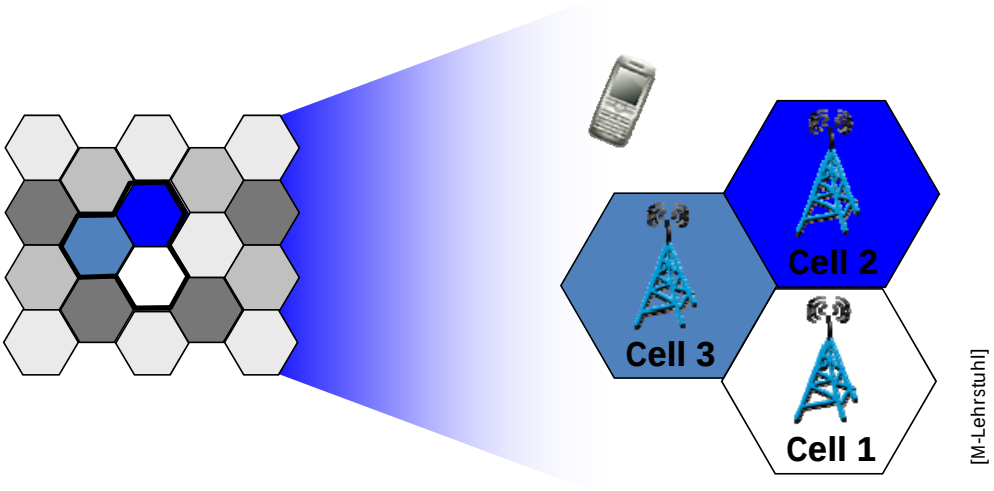

Figure 13: Cell Based Communication (CBC) and cellular communication networks.

The geographic location of the cell's base station/transmitter is well-known and can be used as a point of reference. The position of the mobile user can be approximately determined by using cell identity information, the distance and the angel between the mobile user and base stations. Until recently this information was exclusively known by the network operator. Meanwhile Google is aiming to use cell information by own cataloguing initiatives.

5.2.1 Cell of origin positioning (COO)

The most rudimentary method is the cell of origin (COO) positioning method. Thereby the location of the base station to which the mobile user is connected is considered to be the location of the user. It is more a looking up in the visitor location register than a positioning. The accuracy of the obtained location data depends on the range of the radio cells. The range of the radio cells can vary from 100 meters in urban areas up to 25 kilometres in rural areas, depending on the size of the network's cell.[17]

[17] Ludden, Brendan et al.: Report on implementation issues related to access to location information by emergency services (E112) in the European Union. Coordination Group on Access to Location information for Emergency Services (C.G.A.L.I.E.S) Final report V1.0., http://cgalies.telefiles.de/cgalies_final.pdf, 2002, p. 49.

5.2.2 Time Difference of Arrival positioning (TDOA)

The Time of Difference of Arrival (TDOA) positioning method is based on at least three (synchronised) base stations, which measure the time difference it takes to receive a signal from the mobile user.[18] This information is used to determine the distance between the user and the position relatively to the involved base stations. The location of the user is determined by using advanced triangulation techniques and cross-referencing the distance-information. Multilateration is commonly used in civil and military surveillance applications to accurately locate an aircraft, vehicle or stationary emitter by measuring the time difference of arrival (TDOA) of a signal from the emitter at three or more receiver sites.

Figure 14: Time Difference of Arrival (TDOC) positioning.[19]

5.2.3 Angel of Arrival positioning (AOA)

The angel of arrival (AOA) positioning method seeks to determine a user's location, based on the angel of the signals sent by user' s mobile device. This is done by determining the direction of propagation of a radio-frequent wave incident on an antenna array. In order to calculate the AOA, TDOA is used at individual elements of an antenna array. From the resulting delays, the AOA and therefore the direction can be determined. Finally, using multiple base stationas and AOA, the geographical location can be determined.

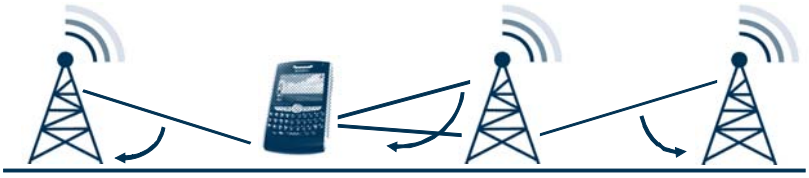

Figure 15: Angel of Arrival positioning (AOA).[20]

[18] Also referred to as multilateration, also known as hyperbolic positioning.
[19] Cf. http://www.gisdevelopment.net/magazine/middleeast/2006/july-aug/22_2.htm
[20] Cf. http://www.gisdevelopment.net/magazine/middleeast/2006/july-aug/22_2.htm

5.2.4 Enhanced observed time difference positioning (E-OTD)

The enhanced observed time difference method (E-OTD) is an improvement of the TDOC method. It measures the time intervals of the radio signals between a base station and the mobile device and a known fixed spot (called location measurement unit). Three location measurement units are needed to determine the position. The mobile device actively participates in the positioning process in contrast to TDOC. E-OTD only works with mobile devices that include E-OTD technology.

Figure 16: Enhanced Observed Time Difference (E-OTD) positioning.[21]

5.3 Accuracy of Location Technologies

The presented technologies for locating a device or a person differ considerably in the way they work. Accordingly, the degree of accuracy with regard to the quality of the positioning has a certain spectrum. Table 1 and Figure 17 give a brief overview of the base characteristics. Furthermore, some of the limitations and possibilities to disturb or manipulate positioning technologies are presented (see Table 1).

[21] Cf. http://www.gisdevelopment.net/magazine/middleeast/2006/july-aug/22_2.htm

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[22], 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[23], Cell-ID.
Other wireless Technologies: **Radio Frequency Identification (RFID), WiFi, Bluetooth**	<1m – 50m	• These 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.
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.).

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

[22] 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.

[23] 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).

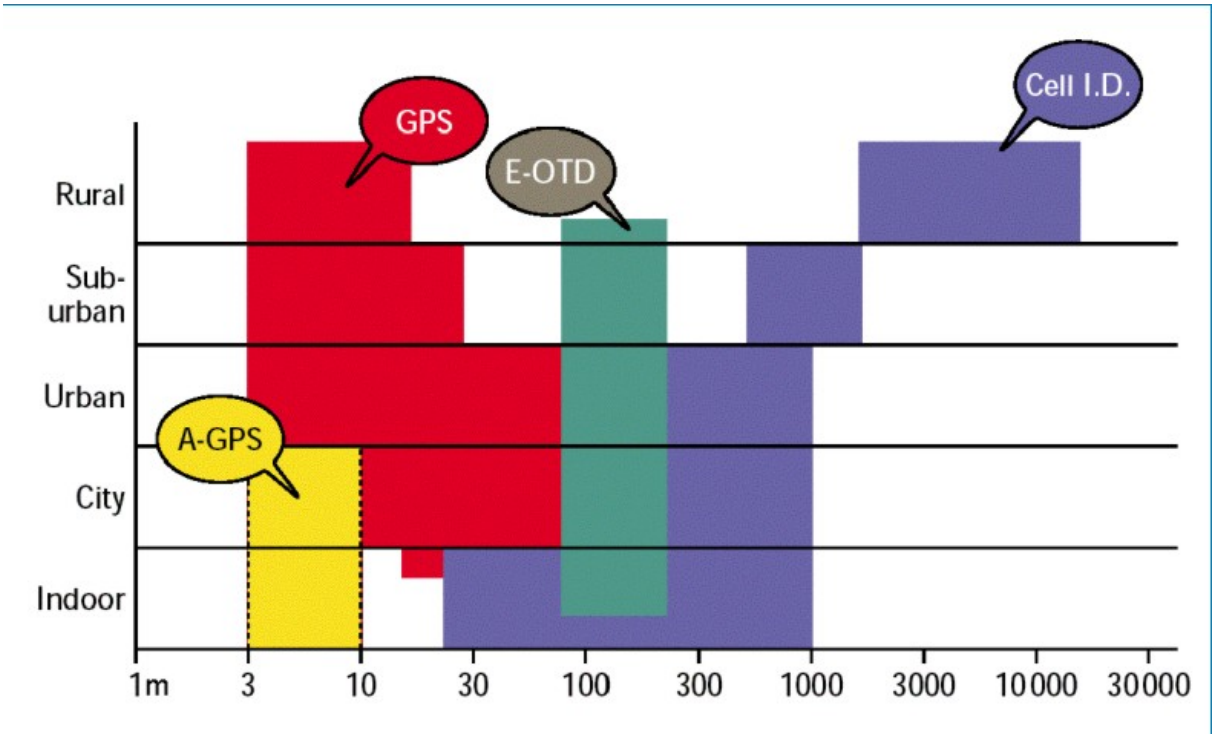

Figure 17: Location Technologies used in Cell-based communication Networks (in GSM: A-GPS, GPS, E-OTD, Cell-ID) and their Accuracy.[24]

[24] Based on <http://nds2.ir.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/mlbs.pdf>.

6 Legal Aspects: The European data protection legal framework regarding Location Based Services

The term Location Based Services appeared in the end of the ’90s and is used for applications that leverage the user's physical location to provide an enhanced service or experience[25], such as route guidance, location of stolen or missing property, tourist and weather information etc. Primary role in Location Based Services play the *location data* that enable the identification of a wireless device. In D11.1: “Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity” we have already made an introduction to the data protection terminology[26], where the terms traffic[27] and location data have been extensively presented.

Location data are “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”[28]. According to recital 14 of the European Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereafter ePrivacy directive)[29] they are data that 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.

Although the ePrivacy directive does not make use of the term ‘Location Based Services’, article 2(g) of the Directive defines the term ‘value added service’ 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’. Therefore a Location Based Service could be defined as a value added service which processes location data other than traffic data for purposes other than what is necessary for the transmission of a communication or the billing thereof. The use of the term ‘location data other than traffic data’ has created some confusion among the legal scholars. In simple word this term refers to all location data that are not used for the transmission of a communication or for setting up a connection (these data are treated as traffic data). A more detailed analysis is contained in FIDIS deliverable D11.5.[30]

[25] http://forum.nokia.com/main/resources/technologies/location_based_services.html
[26] Chapter 5.1 Introduction to the European Legal Framework on Data Protection
[27] Art. 2 (b) ePrivacy Directive “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”.
[28] Art. 2 (c) ePrivacy Directive
[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. L201,37, 31 July 2002
[30] Cuipers, Colette; Roosendaal, Arnold; Koops, Bert-Jaap (eds.): ’11.5: The legal framework for location-based services in Europe, FIDIS deliverable WP11, 2007.

6.1 Legitimate processing of location data for the provision of a Location Based Service

The ePrivacy directive in Article 9(1) allows the processing of location data for the provision of Location Based Services only "when they are made anonymous, or with the consent of the *users* or *subscribers* to the extent and for the duration necessary for the provision of a value added service". In simple words when the data are not made anonymous, the user or the subscriber of the mobile device shall give their consent[31] to the processing of the location data in order to enable the provision of the Location Based Service. However, even when the consent of the user or subscriber has already been obtained, the user or subscriber must continue to have the possibility, using a simple means and free of charge, to refuse the processing of such data for each individual request[32]. When the user initiates the service by calling for instance a number or sending an SMS this action shall amount to consenting to being located.[33]

The directive is not clear whether it is the user who shall give his consent or the subscriber. In most of the cases the subscriber to the service is also the user of the mobile device, so no problem actually appears. However things get more complicated when the two aforementioned attributes are not met in the same natural person, such as in the cases of localisation of employees, of minors or even of people that need assistance in using the mobile device. The use of Location Based Services by the car insurers in order to monitor the movement of the insured has also interesting implications and will be presented below.

Usually, the person to whom the location data relate shall be the one who gives his consent[34]. Sometimes the relationship between the user and the subscriber raises questions whether the consent is freely given, e.g. within the processing of workers' personal data by the employer. In the example of enterprise services the employer is the subscriber, while the employee is the user. Respect to data protection principles would suggest that the person whose consent is needed for the processing of location data is the one whose data are actually processed: the employee (*user*). However in some cases the employer has a legitimate interest to know where the employee is during his working hours (e.g. the owner of a delivery company who has for instance a legitimate interest to know where the driver of a company track is). In such cases it is the employer the one to consent to the localisation of the mobile device when the device is used for working purposes and has the obligation to inform the employee about this.

Similar thoughts, even if not pertaining directly to Location Based Services can be deployed for several activities that include the processing of employee's location data by the employer. Such purposes can vary from the need to improve the distribution or organisation of the work

[31] Consent by a user or a subscriber corresponds to the data subject's consent (Art. 2(f) and Recital 17 ePrivacy directive) as it is defined in the Art. 2(h) Data Protection Directive, that is 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.".
[32] Article 9(2) ePrivacy directive
[33] Idem, p. 6
[34] Article 29 – Data Protection Working Party, Opinion on the use of location data with a view to providing value-added services, adopted on 25 November 2005, 2130/05/EN (WP 115), p. 6

to the surveillance of the use the employees make of the company's means. Such processing raises two issues: the dividing line between work and private life and the degree of acceptable monitoring and surveillance of the employees. Processing location data can be justified where it is done for the planning of operation in real time but not anymore where it is done for the sole purpose of monitoring an employee's work where it can be achieved by other means (WP29, WP115: 10). A balance needs to be struck between the interests of the employer and the workers with the aim to avoid a disproportionate control upon the latter.

The employer should make sure that the processing is really necessary vis-à-vis the purpose and that it can not be reached by other means less intrusive or more "fundamental rights-friendly". Therefore, 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, this processing will only be justified whenever the purpose of the processing can not be achieved by any other means less intrusive for fundamental rights.

Issues of the same kind have been raised with regard to a special kind of Location Based Services, the so-called passive Location Based Services. Passive Location Based Services are defined as those services where a mobile phone user, once he has enabled the service, consents to be located by another, when that other person initiates a location request either from another mobile phone or from a PC[35]. Very popular are the so called Child Location Services that allow the parents to track their children[36]. The Working Party 29[37] identified a series of questions which should be taken into account for further consideration. The fear of parents for criminal offences and the emergence of a nomadic way of living could lead the 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.

In the UK, several mobile network operators and location service providers developed a Code of Practice for the use of passive location services in the UK[38] where it was foreseen that "if the locatee is under 16, the parent or guardian must give consent to the child signing up to the

---

[35] 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

[36] The company SK Telecoms has created and recently launched in the market a cellular phone designed specifically for kids. The phone has a built-in GPS unit that will allow parents to track down the location of their kids, even when the phone is turned off. http://www.gizmodo.com/archives/sk-telecom-human-ear-gps-kids-phone-018408.php (28 July 2004). Services like ChildLocate (http://www.childlocate.co.uk/), Family Locator offered as an extra feature of the Disney mobile (http://www.disneymobile.go.com/disneymobile/home.do) are available in the market. More extreme examples may be the GPS-enabled blazers introduced in a school in Japan (http://www.engadget.com/entry/1234000203040158 - 14 April 2005) or a GPS tracking system embedded in the parent's car that reveals the exact location of the under aged child, of more importance in countries where kids under 18 are allowed to drive, like in the United States (http://www.engadget.com/entry/1234000550052710 – 01 August 2005). However an importance issue comes up regarding the drawing of the line between freedom of the child and parental control.

[37] Working Party 29, Opinion 5/2005 on the use of location data with a view to providing value-added services, WP 115, 25 November 2005.

[38] 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

location service. In addition, the child should also consent. If the child does not consent, his or her wishes must not be overridden and the service must not be activated. In the event that the child does not have the capacity to give consent, the consent of the parent will suffice". Even when the *subscriber*, who is in this case the parent or guardian, and not the child (*user*), is the one to give his consent, the Location Based Service shall be offered only when the child agrees to it.

It shall however be mentioned that the need of the parents to monitor the whereabouts of their children should be limited by the right to privacy of the child as mentioned in the Convention on the Rights of the Child[39]. 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 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.

Great interest presents a case of the French Data Protection authority (CNIL)[40], which had to evaluate the processing of location data from a car insurance Company. The Company wanted to introduce a location device into the car of its customers in order to control the compliance to his contractual obligations. This system would have been implemented on a voluntary basis and would have required the previous consent of the insured. This processing has not been authorised by the CNIL on the basis that a processing monitoring all the driver's movements does not comply with the principle of proportionality, as long as it is exclusively implemented for the control of the respect of the contractual obligations of the driver. Besides, it considered that the systematic collection of vehicles' location data with purpose of modulating insurance rates harms the freedom of movement in an anonymous way in unjustified manner.[41] This position has been echoed by the Working Party 29 in its position paper on the e-call initiative.

6.2 Information to be given before the initiation of the Service

Before obtaining the consent, the service provider must provide the individual with specific information regarding the type of location data that will be processed, of the purposes and the duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the Location Based Service (Art. 9(1) ePrivacy dir.). More information needs to be given to the user according to the provisions of the data protection directive[42] and

[39] UNICEF, Convention on the Rights of the Child, 20 November 1989
[40] Commission Nationale de l'Informatique et des Libertés, www.cnil.fr
[41] CNIL, Proceedings 2005-278 of 17 November 2005, refusing the data processing by MAAF Assurances SA based on vehicles' localisation [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].
[42] 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, L 281, 31, 23 November 1995.

the ePrivacy directive. Such information[43] deriving from articles 10 Data Protection Directive and articles 6 and 9 ePrivacy directive is:

- the identity of the controller and of his representative, if any,
- the purposes of processing,
- the type of location data processed,
- the duration of processing,
- whether the data will be transmitted to a third party for the purpose of providing the value-added service,
- the right of access to and the right to rectify the data,
- the right of users to withdraw their consent at any time or temporarily refuse the processing of such data, and the conditions on which this right may be exercised,
- the right to cancel the data.

The information shall be provided by the party collecting the location data for processing. Thus it shall usually be provided by the provider of the value added service, or if this is not possible by the electronic communications operator. The information could be provided either directly each time the service is used or in the general terms and conditions for the value-added service. In the latter case the service provider should make the information available so that the individuals concerned can consult it again at any time and by a simple method, such as via a website or while using the service (e.g. dialling a toll-free number)[44]. In addition, in cases of ongoing processing of location data the individual shall be regularly reminded about the processing of his location data.

6.3 Frequency of localisation and respective consent

Additional questions arise regarding the frequency of the localisation and subsequently the time validity of the consent. The user or the subscriber gives his consent either for one specific operation or in order to be located on an ongoing basis[45]. In the former case of instant positioning of the user, the localisation is initiated on the order given by the user. This order can for instance be given by dialling a specific number in order to get information related to the region where the user is located (such as weather forecast or the location of his nearest pharmacy or gas station). For the provision of this service the location data of the user are needed and the dialling of the specific number by the user is rendered as consent to being localised[46].

[43] The list of the information to be provided can be found in Article 29 – Data Protection Working Party, Opinion on the use of location data with a view to providing value-added services, adopted on 25 November 2005, 2130/05/EN (WP 115), p. 4-5
[44] Idem, p. 5
[45] Idem, p. 3
[46] Idem, p. 6.

More difficulties appear when the continuous or periodical localisation of the user is needed for the provision of the Location Based Services, in order to offer navigation services for instance. Although it is not clear from the directive whether the consent given for all services of the same category is enough or the consent of the user shall be asked before the initiation of every individual request, it seems sufficient to consent once for a category of requests. How cumbersome and even irritating the latter option could become for the user, can be shown if we think of the 'find a friend' example. The provision of this service requires the constant localisation of all 'friends'. However it is most unlikely that users would like to be localised at any moment of their everyday life or to give their consent every time a request from a friend for their localisation is automatically launched or every time they switch on the tracking service. The possibility of switching on and off the service is foreseen in Art. 9(2) ePrivacy dir., according to which "where consent of the users or subscribers has been obtained […], 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". Article 29 Working Party has expressed the opinion that the service providers should 'regularly remind the user that his or her terminal equipment has been, will be or can be located'[47]. Still one basic question remains and is not very easy to be answered: how can it be ensured that the one that gave his consent to being localised is in fact the person using the mobile phone, the person whose location data are processed.

6.4 Emergency calls and Location Based Services

Art. 10 (b) of 2002/58/EC Directive foresees a general exception to the rule of previous consent for the processing of location data for emergency calls. National organisations dealing with emergency calls and recognised as such are entitled to override the temporary denial or absence of consent of a subscriber or a user for the purpose of responding to such calls. This provision echoes Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (the 'Universal Service Directive')[48] which requires public telephone network operators to make caller location information available to authorities handling emergencies, to the extent technically feasible, for all calls made to the single European emergency call number 112.

In this field, the "e-call" initiative promoted by the European Commission should be mentioned. This initiative aims at introducing a harmonised pan-European in-vehicle emergency call service. For 2010, all new vehicles should have this service as a standard option. As defined in the European Commission Recommendation of 25 July 2003, 'emergency service' means a service, recognised as such by the Member State, that provides immediate and rapid assistance in situations where there is a direct risk to life or limb,

[47] Idem, p. 7
[48] Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (the 'Universal Service Directive), O.J. L108,51, 24 April 2002

individual or public health or safety, to private or public property, or the environment but not necessarily limited to these situations.[49]

The eCall consists of two elements: a pure voice (audio) telephone call based on 112 and a minimum set of data. The eCall (data & voice) carried through the mobile network, is recognised by the mobile network operator as an 112 emergency call. Based on the 112 handling procedure, the operator enriches the call with the caller line identification, and, adds the best location available. This information is transmitted to the appropriate public safety answering point, i.e. the public authority or private service provider operating under the responsibility of a public authority, which is in charge of organising the emergency service (WP29, WP125: 3).

The minimum set of data consists of the time of incident, precise location including direction of driving, vehicle identification, eCall qualifier giving the severity of the incident (as a minimum, an indication if eCall has been manually or automatically triggered) and the information about a possible service provider.

Several data protection issues have been raised by the Working Party 29.[50] First of all, the safeguards should be adapted depending on whether the service is optional or obligatory. In the first case, the Working Party 29 recommends that the device should only be activated upon the request of the user or when a crash occurs in order to enable the data subject to act on a case-by-case basis. Moreover, it should only record limited location data. The Working Party 29 highlights the fact that pressure from insurance car companies or car rental, as well as the obligation put on employees using company cars, to keep the device constantly activated should be considered as illegal.

Regarding the grounds that legitimate the processing, it reminds that even if in many cases, the data processing may be justified by the protection of a vital interest of the data subject (Art. 7 (c), (d), (e) of 95/46/EC Directive), and thus will not required its previous consent, it will no be supported by these grounds in any case. For instance, accidents which do not require the intervention of emergency services might occur and thus activate the device automatically.

In case the activation of the system will be mandatory, the Working Party 29 recommends the enactment of a whole set of rules which should be properly justified in terms of data protection, particularly with regard to the principle of proportionality. It advocates for the use of privacy enhancing technologies in order to empower the data subject to choose his own level of privacy protection.

Another privacy concern arises with the possibility of offering value-added services besides the emergency services. This second level of service lies in adding to the exchanged “basic”

[49] European Commission, Recommendation of 25 July 2003 on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services, O.J. 29 July 2003, L189, p49-51.
[50] Working Party 29, Opinion on the use of location data with a view to providing value-added services, WP 115, November 2005.

information, additional information held by a third party providing added value services, e.g. insurance companies, automobile call centres, medical companies, lawyers, motor clubs, etc. For this it would be necessary to broaden the type of data contained into the minimum set of data. The user would allow the service provider to receive the additional data related to the incident or to the vehicle's occupant. This specific scenario raises the problem of proportionality of the data transferred to the third party for other purposes than the strict provision of the emergency service. "En-bloc" transfers should be avoided and it must be ensured that each third party provider only receives those data that are required for the purposes of the respective contract, etc. Specific provisions should also be taken to cover the cases when sensitive data are processed.

A third concern consists of the creation of databases with the purpose to avoid misuse or abuse of the system in relation to the access by third parties and to possible secondary uses of the personal data transferred. These databases are foreseen to link the car owner's identity and the SIM card of the eCall system and to allow the tracking of the misusing system. This will be possible either by requiring the mobile network operator to identify the owner of the device, as is the case for 112 calls, either by requiring the identification of the authority controlling the Vehicle Identification Numbers.

6.5 Storage and retention of relevant data

The location data used for the provision of a Location Based Service shall be processed only to the extent and for the duration necessary for the provision of the service[51]. After that they should be deleted or made anonymous. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication.[52] However the aforementioned providers may process traffic data for the provision of value added services, if the subscriber or user to whom the data relate has given his prior consent[53]. A highly debated issue is how the prior given consent can be expressed. 'Some form of communication whereby the individual knowingly indicates consent'[54] (opt-in) is essential.

Additionally to these provisions the European Union adopted a directive in 2006 that asks for the retention of specific types of traffic and location data in order to ensure that they are available for the purpose of the investigation, detection and prosecution of serious crime; the directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks

[51] Article 9(1) ePrivacy directive
[52] Art. 6 (1) ePrivacy directive. Exceptions are foreseen for the retention of traffic (and location data) for the purpose of the investigation, detection and prosecution of serious crime see analytically infra.
[53] Art. 6 (3) ePrivacy directive
[54] UK Information commissioner, Guidance to the privacy and electronic communications (EC Directive) Regulations – Part 1: marketing by electronic means, v3.0 (May 2004), p. 5, available online at http://www.ico.gov.uk/documentUploads/Electronic%20Communications%20Part%201%20Version%203.pdf (accessed 17 November 2005)

and amending Directive 2002/58/EC (hereinafter 'data retention directive')[55]. Every Member State can choose to retain these data for periods of not less than six months and not more than two years from the date of the communication[56].

The data retention directive includes a list of traffic and location data, some of which are relevant to Location Based Services and shall be retained after the provision of the service for the competent national authorities to access for law enforcement purposes. Such data can be data necessary to trace and identify the initiator of the Location Based Service and the recipient (in case of Services that include a recipient, such as the Find a Friend service), the data revealing the date and time of the start and the end of the service and the data necessary to identify the type of communication and the location of the mobile communication equipment.

[55] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L105, 54, 15 March 2006.
[56] Art 6 data retention directive

7 Summary and Outlook

Mobility and LBS play an increasing role in everybody's life. Some years ago, the ability of user tracking and tracing was a privilege of governments and extremely determined and resource-full partners. The technologies that are described under 5.1 (network-internal positioning methods) are a result of the technological developments necessary to enable mobile communication services. Especially the cell architecture of the communication networks allows to identify and to localise single users. Thus, the ability of network-internal positioning is in the hands of a few market players per country.

Tracking and tracing using network-internal technologies can be understood as a by-product of providing mobile telephony and data services. But network-external positioning methods also gain additional attention. Mobile devices are increasingly featured with modules that allow to use network-external information sources like GPS, Bluetooth or W-LAN to determine their position.

Following up on the new technological opportunities, new economies and products appear on the horizon: New entertainment services like mobile friend finders (cf. Chapter 3.2) or mobile social communities provide new dimensions of human interaction. But LBS also influence the efficiency of classical value chains and the identity of their employees as it is shown e.g. in Scenario 3: Tracking in the Working Context (cf. Chapter 3.3). Chapter 4 has shown that LBS can have major impact on the mobile identities and that the control of the mobile identities can depend on the properties of the LBS.

Tracking and tracing is becoming more and more a commercial product. The providers of such services are obliged to fulfil the legal requirements with regard to the users' privacy. Although many data protection aspects are covered by the European data protection laws the technical evolution comes along with an evolution of possible privacy threats (cf. Chapter 6), especially since the legislator can react solely to foreseen or already present situations. The responsibility for the users' privacy and the protection of their identity thus rests also in the hand of the providers of LBS. A shift of responsibilities between public and private players with regard to data protection and identity management duties is possible. In this situation, the ability of users' to control their privacy and identity is a major aspect.

The development of the new markets and products give reason to further observe the legal, the technological and the market situation that determine the further / future impact of LBS on users' mobile identities. This will be further pursued in the context of FIDIS Work Package 11 in deliverables D11.6 and D 11.12.

8 Bibliography

Article 29 – Data Protection Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context', adopted on 13 September 2001 (WP 48), available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf

Article 29 – Data Protection Working Party, Opinion on the use of location data with a view to providing value-added services, adopted on 25 November 2005, 2130/05/EN (WP 115), p. 5, available online at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

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

Cuipers, Colette; Roosendaal, Arnold; Koops, Bert-Jaap (eds.): '11.5: The legal framework for location-based services in Europe, FIDIS deliverable WP11, 2007.

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, L 281, 23.11.1995, p. 0031-0050

Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (the 'Universal Service Directive), O.J. L108,51, 24 April 2002

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. L201,37, 31 July 2002

Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L105, 54, 15 March 2006)

European Commission, Recommendation of 25 July 2003 on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services, O.J. 29 July 2003, L189, p49-51.

Ludden, Brendan et al.: Report on implementation issues related to access to location information by emergency services (E112) in the European Union. Coordination Group on Access to Location information for Emergency Services (C.G.A.L.I.E.S) Final report V1.0., http://cgalies.telefiles.de/cgalies_final.pdf, 2002.

Nabeth, Thierry; Hildebrandt, Mireille (eds.): '2.1: Inventory of topics and clusters, FIDIS deliverable WP2, 2005.

Reichwald; Meier; Fremuth: Die Mobile Ökonomie – Definition und Spezifika, in: Mobile Kommunikation, Gabler, Wiesbaden 2002, 4-15.

Royer, Denis (ed.): '11.1: Collection of Topics and Clusters of Mobility and identity – Towards a Taxonomy of Mibility and Identity, FIDIS deliverable WP11, 2006.

UNICEF, Convention on the Rights of the Child, 20 November 1989, available online at http://www.ohchr.org/english/law/pdf/crc.pdf

UK Information commissioner, *Guidance to the privacy and electronic communications (EC Directive) Regulations – Part 1: marketing by electronic means*, v3.0 (May 2004), available online at http://www.ico.gov.uk/documentUploads/Electronic%20Communications%20Part%201%20Version%203.pdf (accessed on 17 November 2005)