FIDIS

Future of Identity in the Information Society

Title:	"D11.3: Economic aspects of mobility and identity."
Author(s):	WP11
Editors(s):	Denis Royer (JWG, Germany)
Reviewer(s):	Jozef Vyskoc (VaF, Slovakia) Mark Gasson (University of Reading, UK)
Identifier:	D11.3
Type:	[Deliverable]
Version:	1.00
Date:	Wednesday, 02 July 2008
Status:	[Final]
Class:	[Public]
File:	fidis.d11.3.economic.aspects.doc

Summary

The markets for mobile communications have been investigated intensively by scientists and market research institutions in the past years. Given the plethora of new services and the sensitivity of the data processed, mobile identity management (MIdM) is needed as an enabler technology to facilitate new services and to offer an effective tool for privacy and data protection.

Extending the previous discussions and findings in the context of FIDIS Work Package 11 on mobility and identity, this deliverable focuses on the economic aspects of mobility and identity. To this regard, topics such as user trust building and the relevant theories for adoption of technologies are explored. Furthermore the perspective on user centric markets and the economic implications from data protection legislation are discussed. Based on the previously discussed topics, initial ideas for an evaluation framework are presented.

Copyright Notice:

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

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (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 Katholieked Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	07/2006	• Initial release (Denis Royer)
0.2	09/2006	• Added contributions by ICPP and K.U. Leuven
0.3	02/2007	• Updated document • Adjustments of Chapter 4
0.4	03/2007	• Updated formatting • Restructuring of the outline → reorganisation of the chapters 3, 4, and 5
0.5	09/2007	• Added initial outline of chapter 5 and 6 by JWG
0.6	10/2007	• Added feedback of Research Meeting 2008 and Work Package 11 meeting • Finalised structure
0.7	05/2008	• Update of document • Extended Chapter 5
0.8	20.06.2008	• Added introduction and conclusion
0.9	30.06.2008	• Finalised Chapter 6 • Edited Executive Summary to reflect the structure of the document • Review version
1.0	02.07.2008	• Final delivery version, incorporating review comments

Contributing Partners:

1. ***JWG:*** Goethe University Frankfurt (Germany)
2. ***VUB:*** Vrije Universiteit Brussel (Belgium)
3. ***ICPP:*** Unabhängiges Landeszentrum für Datenschutz (Germany)
4. ***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(s)*
Reviewer	Jozef Vyskoc (VaF, Slovakia) Mark Gasson (University of Reading, UK)
1. Executive Summary	Denis Royer (JWG, Germany)
2. Introduction	Kai Rannenberg (JWG, Germany) Denis Royer (JWG, Germany)
3. User Centric view on Markets for Mobile Applications and Services: The Four Sector Model	Dr. Martin Meints (ICPP, Germany)
4. Economic Impact of Data Protection on Markets for Mobile Applications and	Eleni Kosta (K.U. Leuven ICRI, Belgium) Nikolaos Volanis (K.U. Leuven ICRI, Belgium)
5. Theories for User Acceptance in the Market of Mobile Identity Management	Denis Royer (JWG, Germany) André Deuker (JWG, Germany) Els Soenens (VUB, Belgium) – Chapter 5.3.3.4
6. Derived Framework	Denis Royer (JWG, Germany)
7. Conclusions	Kai Rannenberg (JWG, Germany) Denis Royer (JWG, Germany)
8. Bibliography	All

Table of Contents

Table of Figures

1 Executive Summary

1.1 Scope

This document is primarily aimed at an audience of academics, EU policy-makers, experts in the fields of economy, law, sociology, technology, and interested citizens. Extending the discussions and findings in FIDIS Work Package 11 on mobility and identity (FIDIS deliverables *D11.1*, *D11.2*, and *D11.5)*, this deliverable focuses on the economic aspects of mobility and identity.

To this regard, topics such as user trust building and relevant theories for adoption of technologies are explored. Furthermore the perspective on user centric markets and the economic implications from data protection legislation are discussed. Based on the previously discussed topics, initial ideas for an evaluation framework are presented.

1.2 Structure and Content

Mobile Identity Management (MIdM) with all its facets is becoming ever more important for today's organisations and users. Increasingly more new services and applications scenarios are being discussed and introduced into the market, offering individuals the possibility to interact with other people or organisations via mobile communication networks in an easy and convenient way. The resulting markets for mobile applications and services and their underlying mechanisms have been investigated by scientists and market research institutions in the past years and various contributions to their understanding were made in both the scientific and practitioner's literature.

As initially discussed in FIDIS deliverables *D11.1*, *D11.2*, and *D11*.5, *user centricity* can be considered an important factor for mobility and identity and the services being used in this context. Consequently user centricity plays a major role in this report. Starting from this notion, ***Chapter 3*** discusses the *four sector model* for communicational contexts (governmental, work-related, public, private), established in social science, by which markets for existing mobile solutions, from the perspective of the user of a mobile device, are categorised. In general, markets are distinguished into inner-sector and cross-sector mobile applications and services. While established processes are important when the governmental and work-related contexts are involved, recent trends and fashions becomes a driving force for applications and services that are going to be used in the public sector (or at least in a public environment). In addition for inner- and cross-sector solutions questions of identity and identity management become important. This is especially true when the private communicational context is affected.

Chapter 4 analyses the legal perspective and the requirements from data protection legislation and other compliance related statutes towards mobile services and applications. To this regard, the user control perspective can be considered an integral part of data protection and is therefore discussed in this context. As discussed in earlier chapters, it can be assumed that the more control over their privacy users can achieve on their own, the fewer external protection mechanisms may be necessary. Accordingly, the data protection discussion shows that Mobile Identity management (MIdM) and Identity management (IdM) are useful instruments to support privacy protection (cp. Chapter 4.7). At the same time the domain of mobile markets is creating a major need for privacy protection, especially due to its extensive use of location information as a basis for basic communication functions as well as a basis for location based services and applications.

Following up on the user-centric markets and the compliance/law perspective, ***Chapter 5*** starts with the analysis of the relevant players in the market for mobile applications and services. These can be arranged into value chains, which are suitable for illustrating value-adding activities among the individual players. For the analysis undertaken here, the players of note for the value chain are (1.) *mobile operator*, (2.) *the service provider* (e.g. for LBS applications and services) and (3.) *the users/customers*. Furthermore, relevant economic theories that help to better understand the adoption and trust building mechanisms of customers and end-users using mobile services and applications are discussed, in order to explain the relevant market mechanisms. These theories include:

- The Theory of Reasoned Action (TRA) → (Chapter 5.3.1)
- The Technology Acceptance Model (TAM) → (Chapter 5.3.2)
- The Diffusion of Innovations (DoI) → (Chapter 5.3.3)
- The Price of Convenience (PoC) → (Chapter 5.3.4)

Furthermore, requirements for continuous trust building are presented that should help organisations to streamline their product and service development efforts for mobile applications. These theories offer a starting point to analyse the impact of MIdM technology, legislation, and customer behaviour towards the customers' acceptance to use a newly introduced technology or service. While explaining acceptance and trust into new services is important, other aspects also play a vital role. When providing mobile applications and services, information is important as well, as it is provided in a non-static but interactive and real-time way, integrating the contextual aspects into the communication between the different players. While an effective use of the provided data offers a higher convenience from services tailored to the needs of users, this also can result into issues with regard to the privacy and security aspects. Consequently, the balance between convenience of service provision and security/privacy becomes an aspect to be investigated. Here, the PoC model offers an explanatory model to better understand the decision processes from the customers' perspective.

However, in order to include all relevant aspects, new and extended models seem to be necessary. In order to combine the previously discussed aspects (markets, compliance/law, and economic theories) ***Chapter 6*** proposes initial ideas for a framework which can give a holistic view on MIdM technology from various relevant perspectives. Here, an approach similar to the balanced scorecard concept, which is developed and widely used for decision support and performance measurement, is taken, in order to combine the different perspectives on MIdM and mobile services and to overcome some limitations of the theories being introduced in Chapter 5. Derived from TAM, PoC, and TRA, the driving parameters/factors for the explanation of the adoption and trust building seem to be: (1.) trust, (2.) usefulness, (3.) ease of use, (4.) convenience, and (5.) privacy. These evidently should be included when analysing markets for mobile application and especially the user/customer perspective. Other relevant perspectives are the technology perspective, the market perspective, the environment perspective, and the law/regulation perspective, which are linked to the strategies of an analysed product and service.

Using this framework mobile operators and service providers should get the opportunity to streamline their product development efforts for mobile applications and to offer better products and services tailored towards the needs of users and customers. However, future

research should focus on the possibilities to apply the proposed framework, the identification of relevant factors, and the identification of their interconnections on each other.

Chapter 7 summarises the findings and gives an outlook on further research opportunities and developments in the market for mobile applications and services. Due to the decline in the revenues for classical, voice-based communications the telecommunications industry is driven towards new business models offering new possibilities to generate profits. However, such newly built services should be built towards the customers' needs in order to be successful. Also, such new services need infrastructure such as the SIM card to manage mobile identities or to offer services such as for payment via the mobile phone or for authentication towards accounts. These aspects will be discussed in the context of the ongoing work of FIDIS Work Package 11.

2 Introduction[4]

Mobile Identity Management (MIdM) with all its facets is becoming ever more important for today's organisations and users. Increasingly more new services and applications scenarios are being discussed and introduced into the market. These markets and their underlying mechanisms have been investigated by scientists and market research institutions in the past years and various contributions[5] were made in both the scientific and practitioner's literature.[6]

Extending the discussions and findings of FIDIS Work Package 11 on mobility and identity, this deliverable focuses on the economic aspects of mobility and identity. As initially discussed in FIDIS deliverables *D11.1*, *D11.2*, and *D11.5*[7] *user centricity* can be considered an important factor for mobility and identity and the services being used in this context. Consequently user centricity plays a major role in this report.

The report is divided into 7 main chapters, whose structure and content is further visualised in Figure 1. Following the introduction (***Chapter 2***) and starting from the notion of user centricity, ***Chapter 3*** discusses the *four-sector-model*. This model categorises existing mobile solutions from the perspective of the user of a mobile device in order to motivate the need for privacy and security of communication within and across the borders of the individual sectors.

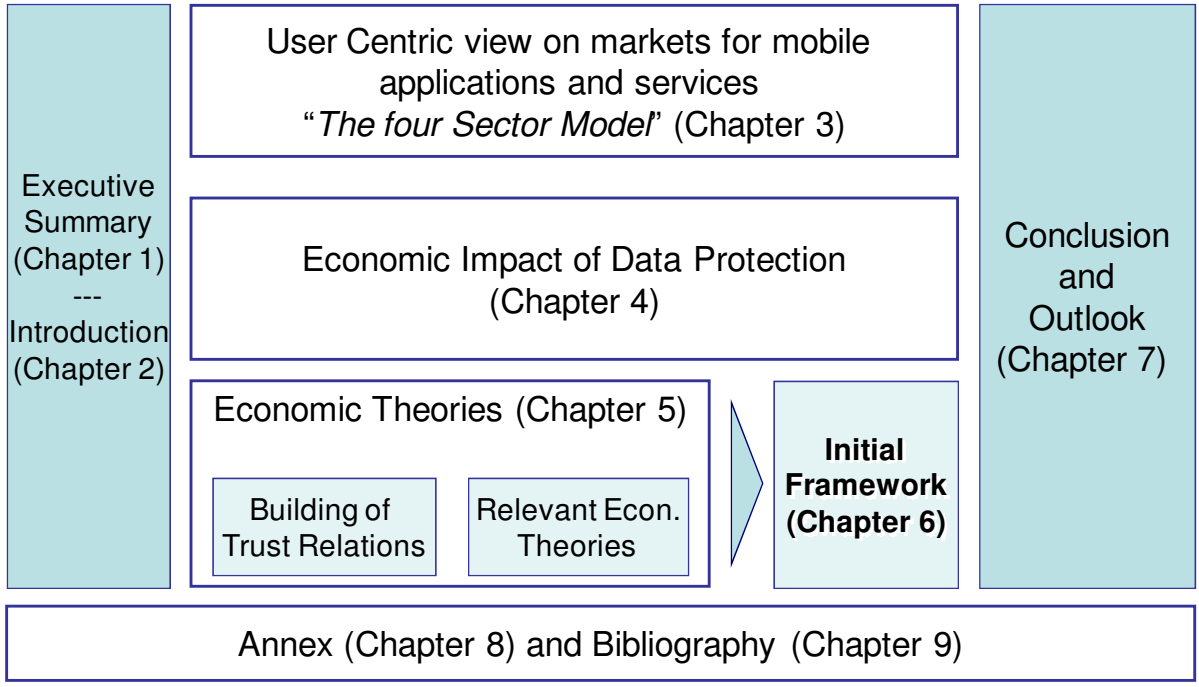

Figure 1: Structure of FIDIS deliverable D11.3

Chapter 4 analyses the legal perspective and the requirements from data protection legislation and other compliance related statutes towards mobile services and applications. To this

[4] Contributed by: Denis Royer and Kai Rannenberg (both JWG, Germany).
[5] Cf. Ngai, E. W. T. and Gunasekaran, A., 2007.
[6] E.g. Büllingen,F., Stamm, P.,2004; Nohria, N., Leestma, M., 2001; Rebne *et al.*, 2002; Ristola *et al.*, 2005; Roussos et al, 2003; Siau, K., Shen, Z., 2003.
[7] Please visit http://www.fidis.net/resources/deliverables/mobility-and-identity/ for further details on the work of FIDIS Work Package 11.

regard, the user control perspective can be considered an integral part of data protection and is therefore discussed in this context.

Resulting from the discussion in the previous chapters it can be assumed that the more control over their privacy users can achieve on their own, the fewer external protection mechanisms maybe necessary. Accordingly, the data protection discussion shows that Mobile Identity management (MIdM) and Identity management (IdM) are useful instruments to support privacy protection (cp. Chapter 4.7). At the same time the domain of mobile markets is creating a major need for privacy protection, especially due to its extensive use of location information as a basis for basic communication functions as well as a basis for location based services and applications (cf. FIDIS deliverable D11.2[8]).

Following up on the user-centric markets and the compliance/law perspective, ***Chapter 5*** discusses the relevant economic theories that help to better understand the adoption and trust building mechanisms of customers and end-users using mobile services and applications. Furthermore, requirements for continuous trust building are presented that should help organisations to streamline their product development efforts for mobile applications. These theories offer a starting point to analyse the impact of MIdM technology, legislation, and customer behaviour towards the customers' acceptance of a newly introduced technology or service.

In order to combine the previously discussed perspectives (markets, compliance/law, and economic theories) ***Chapter 6*** proposes initial ideas for a framework which can give a holistic view on MIdM technology from various relevant perspectives. Here, an approach similar to the balanced scorecard concept is taken, in order to combine the different perspectives on MIdM and mobile services and to overcome some limitations of the theories being introduced in Chapter 5.

Chapter 7 summarises the findings and gives an outlook on further research opportunities and developments in the market for mobile applications and services.

[8] Cf. Deuker, A. (ed.), 2008.

3 User Centric view on Markets for Mobile Applications and Services: The Four Sector Model[9]

3.1 Introduction

The market for mobile computing solutions has been investigated intensively by scientists[10] and market research institutions[11] in the last years.[12] In most cases the research takes the perspective of vendors of products and solutions or organisations introducing mobile computing., From these perspectives, business processes and workflows that benefit from the use of mobile solutions (internal business or business to business perspective) are especially investigated as they seem to be the most promising market.

Based on the work of Bergmann, Rost and Pettersson,[13] in this chapter a different perspective is taken: that of a user of a mobile device taking various roles within society in different communicational contexts. Notably, the communicational contexts and the corresponding roles taken by the participants define their partial identities. So this perspective is also an (partial) identity centric view on markets for mobile applications and services.

Following the theory of social systems which is a contribution of sociologists to systemics, roles can be assigned to two social systems:

- *Interactional systems* (types of communities in which members are not subject to particular rules, but nevertheless schemes apply - examples are spontaneous meetings as neighbours, spontaneous encounters)[14]
- *Organisational systems* (characteristics are membership and effective production of decisions - examples are public bodies, institutes and companies)[15]

While roles in interactional systems show a big variety, organisations mainly distinguish between members (such as employees) and clients (such as customers or citizen). These aspects have been elaborated in detail.[16]

Bergmann, Rost and Pettersson developed the model of the virtual city as paradigm for user interfaces for mobile devices. They clustered communicational contexts and mapped them to three areas of a virtual city: public area, business related area (i.e. the user's work zone), and private area. As the virtual city model was not developed to analyse markets for mobile solutions, clusters of applications we can find there or the corresponding privacy and security needs, it is limited when addressing the following aspects:

---

[9] Contributed by: Dr. Martin Meints (ICPP, Germany).
[10] Such as the research groups at the University Hamburg (see http://www1.uni-hamburg.de/m-commerce/) or at the University of St. Gallen in Switzerland (see http://verdi.unisg.ch/org/iwi/iwi_pub.nsf/wwwPublRecentEng/2E693258E01E595DC1256F40003D69DB) and the chair for m-commerce at Frankfurt University (see http://www.m-lehrstuhl.de/)
[11] For an overview of studies carried out by Berlecon Research, the Meta Group Deutschland GmbH and Ubitexx see http://www.computerpartner.de/knowledgecenter/mobilecomputing/224911/
[12] Cf. Ngai, E. W. T. and Gunasekaran, A., 2007.
[13] Cf. Bergmann, M., Rost, M., Pettersson, J. S., 2005.
[14] Cf. Kieserling, A., 2000.
[15] Cf. Baecker, D., 1999 and Luhmann, N.,2000.
[16] Cf. Nabeth, T., Hildebrandt, M. 2004 and Koops *et al.* 2006.

- The public sector in the virtual city model integrates, due to the similarity to a traditional market place, a number of different types of communication and as a result different applications and services. This limits the applicability of this model for classification purposes of applications and products with respect to economic factors.
- The specific nature of governmental communication in difference to communication originating from or targeted at private enterprises cannot be distinguished by different sectors in this model. They all are mapped to the public area in the city model which does not allow for a detailed analysis of the different kinds of communication and underlying applications in this area.

Taking over the user centric view and the focus on communicational contexts from the virtual city model we define in development of the original model four sectors as targets for communication originating from a user of a mobile device:

- The *business related* sector, where any one-to-one (1:1) communication to a private enterprise takes place. In this context we also summarise the individualised part of the communication when using a shop (personal suggestions of what to buy, the shop trolley, the payment etc.). The communication partner is a member (employee) of an organisation.
- The *governmental* sector, where any 1:1 communication with governmental institution and offices takes place. The communication partner is a member (employee) of an organisation.
- *The private sector*, where we have personal social contacts. Communication from the perspective of the user is typically 1:1 or takes place in small groups of trusted persons. The communication partners either take roles in interactional systems or are clients of an organisation.
- *The public sector*, this sector has a different nature as compared to the other sectors. At least one participant of the communication aims at many partners (**1:n communication**) in a public way. Examples for this kind of communication are public parts of online-shops, postings in open web fora, portals, newsletters, scientific online articles, etc. In addition the information published typically is not confidential. The publisher at the moment of publishing does not know exactly which role and in which social system the recipient of the communication will take.

The following figure illustrates the described four sectors:

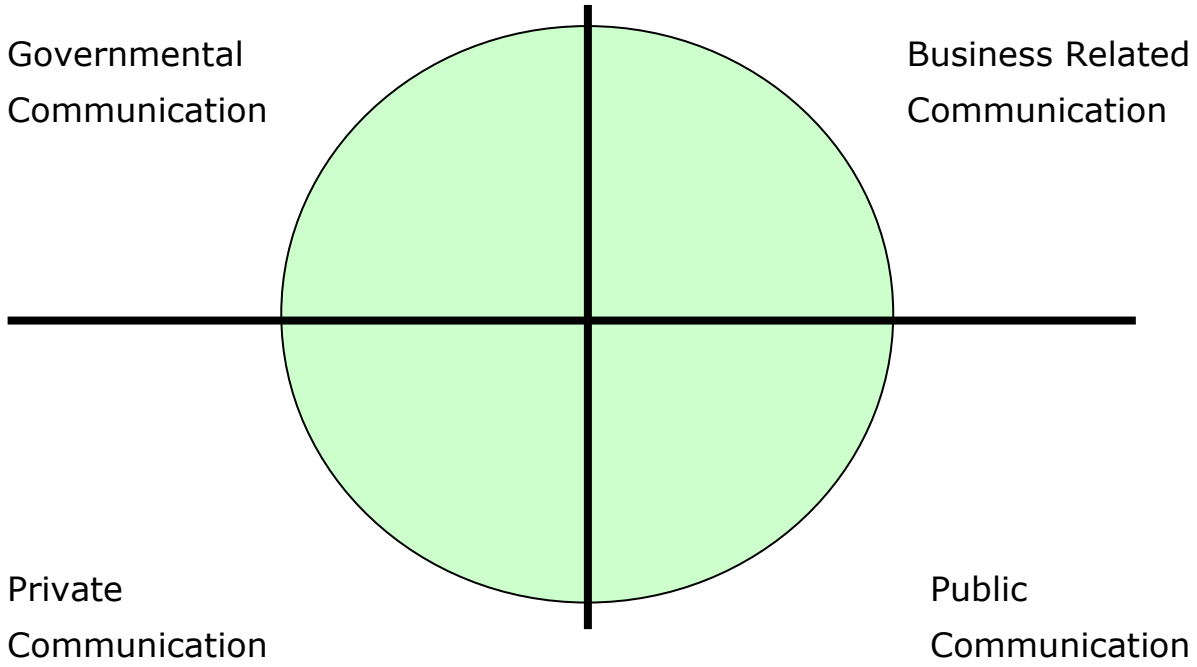

Figure 2: Four sectors of general communicational contexts

The starting point for communication, represented by the role the user of the mobile device is taking, is typically one of the following sectors:

- ***Business related sector*** (role of the user of a mobile device: member (employee) of a private enterprise)
- ***Governmental sector*** (role of the user of a mobile device: member (employee) of a public institution)
- ***Private sector*** (role of the users of the mobile device: various roles in interactional systems or client of an organisation such as citizen or customer). In this case the private character of the communication is not always that precise as many kinds of private communication take place in a public environment for example a restaurant, on the street, etc. and communication is done in the open

The public sector in this model cannot be used as a initial point of communication in a meaningful way because it is very unlikely that many people will start communicating to one organisation at the same time (many 1:1 communications adding up to a n:1 communication). In addition, from a social scientist's point of view one-to-one communication that starts with the initiating communication partner having no role in a social system in mind do not exist.

In general the sectors in the upper half are dominated by organisations. Persons communicating in these two sectors typically take the role of a member of an organisation. In the public sector we find all kinds of roles in the communication. This sector is used by organisations as well as by individual persons. In the private sector individual persons in various roles (clients of an organisation and roles in interactive systems) take part in communication.

This model has limitations especially in the precision these sectors are described with – to the authors the borderline between the sectors seems to be weak. The reason is that many different aspects of communication have to be covered. Examples are:

(1) Different roles in various social systems (including functional systems),

(2) Different type of communication (1:1, 1:n), and in addition

(3) Shifts in roles and type within the communication, which are also possible

3.2 Application of the four sector model

Following this model, we generally can observe two types of communicational relationships:

1. inner-sector communication (only possible in those sectors that can serve as a starting point: business related, governmental and private sector) and
2. cross-sector communication

These will be described and mapped with commonly used descriptions of business relationships such as business to customer (b2c) and commonly used types of communication such as one-to-one or one-to-many (broadcast like) communication. In addition the resulting types of communication are described with respect to their needs for privacy and security. In cases where security is mentioned, the traditional three aspects of security are meant:

- Availability (availability and in case of incidents time for the reestablishment of applications and services)
- Confidentiality (data can be accessed and used by authorised persons only)
- Integrity (data can be modified by authorised persons only. Especially in the context of electronic signatures, non-repudiation and authenticity of the user are important elements of integrity as well)

Privacy protection is understood in a general sense as protection of the private sphere. In addition to data protection this includes the right to be left alone, reachability management and other methods that allow for the protection of the private sphere of an individual.

3.3 Inner-sector communication

3.3.1 The business related sector

Inner-sector communication in this sector contains direct business to business (b2b) communication (type 1:1 communication).

The market for mobile solutions directed to business to business (b2b) communication is investigated in many studies and market surveys[11]. Solutions in this segment are supporting typical inner- and cross-organisational workflows. Examples of existing or emerging solutions are:

- Encrypted e-mail access on mobile devices - these solutions currently seem to be one of the most successful mobile solutions on the market.[17]

[17] See http://www.cio.de/markt/800187/ (accessed on 25 June 2008)

- Mobile access to internal enterprise applications (such as customer relationship applications (CRM), enterprise resource planning systems (ERP), supply chain management (SCM), business intelligence (BI) and knowledge management solutions, etc.)
- Collaboration in projects, data access and exchange (work-grouping)
- Solutions for logistics, tracking and tracing (see also[18])

According to the communicational needs in business processes the type of communication can be one-to-one (1:1) or one-to-many (1: n, broad- or multicast like). Especially in collaborative contexts, 1:n communication is established via e-mailing list or work-grouping solution.

In general security in this sector is important. The reasons are trade secrets and personal data (compliance to data protection legislation) that are processed.

3.3.2 The governmental sector

In our understanding, public institutions include government, universities and, following the situation in most European countries, the health sector as well. The communicational relationships can be of the type one-to-one (1:1) and one-to-many (1:n).

The market for government to government (g2g) mobile solutions currently is restricted, but high-tech oriented and innovative. In this segment mobile solutions are mainly developed for the military[19], police[20] and rescue forces. This includes applications for communication and command support[21], situation and case analysis[22], access to central databases[23] including geographical information systems (GIS)[24], and military logistics.[25] A rarer example is inner-governmental applications for mobile electronic signatures as they are implemented for example in Lithuania.[26]

Following the trend of the business sector, mobile access to strategic governmental applications can be expected in the future. But this might take some time as currently most European governments are introducing non-mobile e-governmental infrastructures and solutions (see for example applications using electronic signatures[27]).

---

[18] Cf. Deuker, A. (ed.), 2008.

[19] See for example http://www.dafu.de/praxis/militaer.html and vendors for example http://de.itronix-europe.com/News/News_Article.asp?id=254, http://www.toughbook-europe.com/DEU/business_kompetenz.aspx and http://www.intergraph.com/military/mobilesolutions.asp

[20] See for example http://www.ipsi.fraunhofer.de/mobile/teaching/seminar-ws0304/BOS_Polizei.pdf and http://www.hessen-media.de/mm/egovernment-in-hessen-CeBIT-2004.pdf

[21] For example ILIAS for the police; see http://www.hessen-egovernment.de/dynasite.cfm?dssid=72&dsmid=1957&dspaid=14090 or for military integrated systems including application see for example http://www.aselsan.com.tr/msting/mobKomKont_eng.htm

[22] For example: CRIME application for police forces in Germany, see http://www.hessen-egovernment.de/dynasite.cfm?dssid=72&dsmid=1957&dspaid=14102

[23] For example: mPol application for police forces in Germany, see http://www.hessen-egovernment.de/dynasite.cfm?dssid=72&dsmid=1957&dspaid=14088

[24] For example an application for police forces and fire brigades see http://usa.autodesk.com/adsk/servlet/item?format=print&id=4621255&linkID=3514346&siteID=123112

[25] Cf. Garfinkel, S., Rosenberg, B., 2005.

[26] Cf. Gudauskaite,S., Peciura, L., 2004.

[27] Cf. Gasson, M., Meints, M., Warwick, K., 2005.

Typically security for these applications (and naturally the whole systems) is very important as the information is generally confidential, e.g. because of the personal data that are processed (for example in police databases and the medical health system) or their military and police related nature (state secrets). In addition the need for availability and integrity of data is high.

3.3.3 The private sector

This kind of communication can be mapped to citizen to citizen / customer to customer (both c2c) communication, but the mapping is not accurate. Parts of c2c communication will also be found in cross-sector communication between the private and the public sector. The reason is that the definition of the borders between these sectors seems to be difficult, as obviously a number of services originating or targeting at the private sector aim at a public recognition. The services for which this is obviously the case will be discussed in the following section.

In addition communication can change its character when proceeding. One typical example is online shopping. The online shop itself is public - anybody can have a look at offers and prices. And having a look at them from the perspective of an individual typically is considered to be a private activity. To achieve this, anonymising services[34] for example can be used. But anonymity typically cannot be kept up when putting goods in the shopping trolley and moving it to the cashier. In this situation today typically personal data is being transferred to facilitate the purchase[28]. The collection of goods in the trolley and the amount and way one pays belong to personal data and are thus subject to data protection. From the perspective of the operator of the online shop, the communication changed its nature from general (1:n) to related to a specific customer (1:1).

In cases of a definite inner-sector communication in the private sector privacy and security becomes an important issue. Typically the communication is of the type one-to-one (1:1), but especially for Location Based Services (LBS) third parties can be involved leading to more complex communicational relationships.

This communicational context shows a large variety of different applications. Examples are Location Based Services (LBS) to track one's own child[29] or, more precisely, to track a mobile device.[30]. But simple private mobile communication to one's spouse belongs to this context as well.

3.4 Cross-sector communication

3.4.1 Communication directed to the public sector

In this chapter we typically have one-to-many (1:n) communication or communication of the one-to-one (1:1) type that has a public nature or aims at public recognition. Typical examples for these types of communication are public WAP[31] or web-portals optimised for mobile access. These portals offer in addition to information services and marketing and sales

[28] For shopping privacy enhanced processes allowing for pseudonymous shopping have been developed. See for example Hansen, M., Krasemann, H., *PRIME White Paper V1*, Kiel, July 2005. Download http://www.prime-project.eu.org/public/prime_products/PRIME-White-Paper-V1.pdf
[29] For example http://www.trackyourkid.de/
[30] For example http://puremobile.de/index.php?cPath=21
[31] WAP: Wireless Application Protocol; an introduction and an overview on a few WAP-portals can be found at http://www.dafu.de/rechts/rechts-wap.html

information traditional internet services such as chat and blogs or new services such as photo galleries.

Two of the most successful mobile services or products in this section are SMS[32] and ring tones[33]. SMS in many cases seems not to be driven by usefulness and cost efficiency only, as with current prices for mobile communication SMS seems to be expensive compared to the content that can be transferred. For both products, recognition in public seems to be an influencing factor, when the service or the mobile device is used. They demonstrate that the success of this market segment is not driven by the technical or procedural usefulness only, but also by fashion. In markets that are driven by fashion the prognosis of mid- or long-term trends is very difficult, the economic risk when entering such markets are high for the vendors and service providers.

As the information in these communicational contexts is at least partially meant to be public, confidentiality is not always an important issue here. But integrity and availability can be important aspects of security nevertheless, as manipulation of information or non availability of services can have economic consequences for vendors and service providers (loss of customers for paid b2c services).

The composition of the targeting group for 1:n communication has an impact on the need for privacy. Privacy can be an important issue in public communicational contexts especially in cases where persons are in a role as client of an organisation. In these contexts we can observe the use of a number of anonymising[34] services in the internet. These services in principle can be used on mobile devices as well. In addition in numerous web fora the use of pseudonyms is very common.

Within the public area we also observe types of communication that are driven by the need for reputation and thus aim at identifiable creators of information and linkability of the publications under the same name (for example in scientific and technical communities).

3.4.2 Business related and governmental sectors

The market for business to government (b2g) and government to business (g2b) solutions currently does not seem to be very well documented. One of the few well known approaches for these types of communications are in addition to simple mobile voice communication mobile electronic signature solutions that are established for example in Finland and Austria (A1 signature[35]). Examples for applications for mobile signatures in these communicational contexts are portals of the public sector for placing of contracts.

Due to the secret nature of the information (for example trade secrets for bargains) or the personal nature of data transferred and processed, security and data protection are important for solutions in theses communicational contexts. In cases of signature based solutions, authenticity and non-repudiation are additional important aspects of integrity. The applied level of security and the corresponding technical and organisational measures are typically defined with the target able to insure against the remaining risks.

---

[32] See for example http://www.nokia.de/de/hintergrundberichte/2002/25540-popupContentArea.html
[33] See http://www.wirtschaftsrat.de/data/landesverbaende/HH/Digitale_Trends11-2004.pdf, p. 9.
[34] For example: AN.ON (http://www.anon-online.de/) or Tor (http://tor.eff.org/)
[35] See http://www.signatur.rtr.at/de/providers/services/mobilkom-a1signatur.html

Potentially the compliance to data protection legislation may be a unique selling proposition (USP) for this type of product and service. In this context privacy seals may be of relevance in the future.

3.4.3 Communication emerging from the private sector

This kind of communication shows a big variety as we have one-to-one (1:1) communication to the business sector (customer to business, c2b) and the government (citizen to government, c2g) and the communication to the public sector already mentioned.

Private enterprises as well as public institutions try to establish communicational contacts to customers or citizen via mobile portals. While we have numerous established business portals for mobile communication run by enterprises[36], the situation for mobile governmental services is different. In Germany we still observe a discussion on strategies[37], in Finland the infrastructure for mobile electronic signatures has been established in 2005[38] and is available for every citizen, though usage seems to increase slowly.[39]

In these communicational contexts privacy is a driving force for security, especially confidentiality and integrity. Typically an individual user can accept a lower level of availability. In many cases individuals without an organisational context do not have the knowledge and currently do not seem to see the incentive to apply even basic security measures such as virus protection and secure configuration of external interfaces on their mobile devices[40]. Practically speaking, the observed need for security and the implementation differ widely. An enhanced automated security management for mobile devices (including for example patch management and virus protection) and more secure default configurations of external interfaces could improve the situation significantly in the future.

3.5 Summary

The four sector model for general communicational contexts introduced offers a systematic approach to understand the need for privacy and security of communication within and across the borders of sectors. Typically security and privacy show certain characteristics in the private, business and government related sector. The need for security and privacy in the public sector shows a certain range, depending on specific communicational contexts. In addition the type of communication (1:1, 1:n and the composition of the group n) has an impact on the levels of privacy and security needed.

The sectors show certain characteristics, each concerning the type of mobile applications that are used (for example specific governmental applications in the governmental sector) and driving forces for the markets within these sectors (for example fashion in the public sector). These characteristics cannot easily be transferred to other sectors. They define directions and borders of future developments of applications within or across the sectors.

---

[36] For example: AOL see http://mobile.aol.com/portal/main.php, or T-Zone http://www.t-zones.de/de/index.html
[37] See for example http://www.egovernment-akademie.de/academy/content/sections/
[38] See for example http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=3337
[39] Cf. Meints, M., Hansen, M., 2005.
[40] See for example http://www.kronegger.at/?url=newsletter-200502a-mobile&lang=en

4 Economic Impact of Data Protection on Markets for Mobile Applications and Services[41]

4.1 Introduction

In the advent of the mobile revolution, identity is facing great challenges. Mobility has freed the subscriber or the user of a service from a specific space, rendering it unclear not only who the person initiating a communication is, but also where this person is located and how many ways he has in order to express a communication. The volume of data generated and processed has proliferated, giving rise to new privacy threats. There is an increasing number of situations in which the user is either not aware that his personal data is collected or his system unlawfully accessed[42] or he chooses to sacrifice it in return for other benefits[43].

'Data processing' is defined as *"*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*"*[44]. It follows that the definition of processing is extraordinarily broad, so that it is difficult to conceive any operation performed on personal data which would not be covered by it. It is important to note that mere storage of personal data by the providers of publicly available electronic communications services or of a public communications network constitutes 'data processing', so that simply storing data on a server or other medium is deemed to be processing, even if nothing else is being done with it.

The broad definition of data processing can lead to uncertainty as to what can be included under processing when it comes to mobility and new technologies. The European Court of Justice has ruled that *"*the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46*"*[45]. Such a broad interpretation of 'data processing' can expand the meaning in the field of mobile communications, imposing extensive obligations on the service providers.

4.2 Rights of the data subject

Although a casual look at the text and chapters of the data protection directive would suggest that the data subject is granted only two rights (right of access and right to object), a closer look reveals that it implicitly grants more rights to the data subjects. This approach is indeed needed to ensure that the data subject remains the ultimate controller of his personal data, a purpose whose fulfilment fortifies the fundamental right to privacy – as it is stipulated in

---

[41] Contributed by: Eleni Kosta and Nikolaos Volanis (both K.U. Leuven ICRI, Belgium).
[42] Cf. IPTS, 2003, p. 29.
[43] Cf. Danezis, G., Lewis, S., Anderson, P., 2006.
[44] Article 2 of 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, hereinafter called 'data protection directive'.
[45] Judgment of the European Court of Justice (6 November 2003), Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping, par. 27

Article 8 of the European Convention on Human Rights (ECHR). The safeguarding of these rights is obligatory according to the European data protection legislation, although it might entail high economic consequences.

In brief, the data protection directive sets forth several specific rights to the data subjects, each one covering a different phase within data processing:

First, the data protection directive considers that the data subject has the **right to know** whether his personal data are being collected and processed. This right is closely related with the consent of the data subject, since the latter is considered as one of the criteria of legitimate processing (after all, the consent of the data subject presupposes a general knowledge of the facts that he is consenting to). However, even in cases where the user has not given his consent (for example, processing is necessary for compliance with a legal obligation to which the controller is subject), the right to know remains in full effect. It follows, that the data controller must still inform the data subject that his personal data are being processed, in accordance with the Articles 10 and 11 of the data protection directive. Moreover, this specific right is mentioned in recital 25 of the data protection directive as a reflection of a good interpretation of the data protection principles.

The data protection directive perceives the information to be provided more as an obligation from the part of the data controller, and less as a specific right of the data subject. When the data are collected form the data subject, the minimum information that has to be provided is the following[46]:

a. the identity of the controller or his representative
b. the purposes of the processing for which the data are intended
c. any further information if this is necessary to guarantee fair processing in respect of the data subject, such as:
    - the recipients or categories of recipients of the data,
    - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of the failure to reply,
    - the existence of the right of access to and the right to rectify the data concerning him.

This information has to be provided to the data subject at the time or before the data is collected. If disclosure to a third party is envisaged, article 11 provides that the information must be provided at the latest when the personal data will be disclosed.[47] For example, in cases where the mobile network provider, acting as the data controller, decides to further communicate the traffic data of his network to third parties to be used for the provision of value added services, he must first acquire the unambiguous consent of the subscribers.

Second, the data subject has the **right to object**[48] to the collection and processing of his personal data. However, this right is overridden by the various exceptions (deemed 'necessary') which are found in article 7 of the data protection directive:

---

46 Article 10 data protection directive

47 Article 11(2) excludes the right of information in cases where the disclosure to a third party is made for statistical purposes or for the purposes of historical or scientific research, and when 'the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by [national] law'.

48 Article 14 and recital 45 data protection directive

a. when the process is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
b. when the processing is necessary for compliance with a legal obligation to which the [data] controller is subject,
c. when the processing is necessary in order to protect the vital interests of the data subject,
d. when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the [data] controller or in a third party to whom the data are disclosed and
e. when the processing is necessary for the purposes of legitimate interests pursued by the [data] controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights for fundamental rights and freedoms of the data subject.

However, article 14 data protection directive stipulates the cases where the right to object can be exerted:

a. At least for the last two aforementioned cases, Member States are obliged to grant the data subject a right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. When there is a justified objection, then the processing instigated by the [data] controller may no longer involve those data.
b. The data subject can object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

The ePrivacy directive[49] perceives the right to object as withdrawal of consent. Therefore, the specific right is implicitly mentioned in Art. 5(3) (cookies), 6(3) (traffic data processed for the purpose of marketing electronic communications services or for the provision of value added services), 9 (processing of location data other than traffic data), 12 (directories of subscribers) and 13 (unsolicited communications). In all the aforementioned cases, the data subject is given the right to refuse the provision of services or in cases where he has already accepted them, to withdraw his consent. As regards the processing of location data in particular, 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, of temporarily

[49] 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, pp. 0037-0047, hereinafter called 'ePrivacy directive'. The ePrivacy Directive replaced Directive 97/66/EC of the European Parliament and the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector, O.J. L 53, 14 January 1998

refusing the processing of such data for each connection to the network or for each transmission of a communication.[50]

Third, article 12 of the data protection directive grants the data subject the **right of access** to his collected personal data, meaning that every individual whose personal rights are been collected and processed has the right to obtain from the data controller:

a. confirmation as to whether or not his personal data are being processed and information at least as to the purposes of the processing, the categories of the data concerned, and the recipients or categories of recipients to whom the data are disclosed,
b. communication to him in an intelligent form of the data undergoing processing and of any available information to the resources and of any available information as to their source.

Where any automated decisions (as defined in Article 15 data protection directive, see *infra*) are involved, the data subject has the additional right to be informed about the logic involved in any automatic processing of data concerning him.

All the aforementioned information must be available to the data subject 'without constraint at reasonable intervals and without excessive delay or expense'[51]. In addition and as regards how the right of access is exercised, an ideal situation would include both online and physical access - the latter realised at the physical address of the data controller. However, in cases where physical access would entail disproportionate efforts and costs on behalf of the data controller (or if the data collected is disproportionately little), it is arguably accepted that the right of access can be exercised only through online means. Considering the various security risks, we would suggest that the data controllers should not provide information unless they can verify the identity of the applicant (e.g. through the use of an electronic signature). This is specifically important in cases where the accidental disclosure to an individual who is impersonating the data subject would be likely to cause damage or distress to the real data subject.

Fourth, the right of access includes a **right to rectify, erase or block** the data that relate to him, in cases where their processing does not comply with the requirements of the data protection directive (for example, the data controller's collection of personal data is disproportionate to his purposes), and in particular when the data at issue are incomplete or inaccurate.[52] That would be the case, for example, when the name of the subscriber to a mobile network is registered wrongly.

Fifth, article 15 of the data protection directive confers to the data subject a **right not to be subject to an automated decision** which produces legal results concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. A statutory exception to this right is provided in 12(2) of the aforementioned directive, in cases where the decision is either:

a. Taken in the course of the entering into or performance of a contract, provided that the request (for the entering or the performance of the contract) has been

50 Article 9(2) ePrivacy directive
51 Article 12 (a) data protection directive
52 Article 12 (b) data protection directive

lodged by the data subject and there are suitable measures to safeguard the data subjects legitimate interests; or

b. authorised by a law that also lays down measures to safeguard the data subject's legitimate interests.

There is no further guidance in relation to the phrase 'significantly affects'. A logical interpretation would associate the verb 'affect' with emotional distress. Therefore, in order for the specific right to be activated, the data subject should suffer significant emotional distress[53]. It does not necessarily have to result in physical damage or financial loss. On the other hand, it would seem unlikely that a data subject will object to receipt of an unsolicited benefit, even if it has occurred because of automated processing (e.g. as a result of automated processing, the data subject is promoted).[54] In the field of mobile communications for example, it is doubtful that this article would be evoked by an employee in a courier enterprise, when, due to the erroneous processing of his location data, he appears to be more productive and therefore he gets a financial bonus.

Sixth, the data protection directive makes it clear that the processing of personal data must be done in a maximum security environment. It therefore calls the Member States to impose a security obligation to the data controller, who must implement '[…] appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing'[55]. In addition, '[h]aving regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected'.[56] This obligation of the data controller can arguably lead to a derivative **right** of the data subject **to know** the **extent to which his data is secured**, which serves as a supplemental right to the general information right of the data subject (discussed *supra*). In brief, the obligations of the data controller regarding the processing of personal data are:

a. establishment of the appropriate standards and procedures,
b. selection of personnel based on their skills and ethics and which has received appropriate training in security issues,
c. management of outsourcing contracts and the selection of a data processor according to the technical and organisational security measures governing the processing.[57]

In relation to the last security obligation, the directive provides that when the carrying out of data processing is performed by a data processor, it must be governed by a contract or legal act which binds the processor to the controller and that specifically stipulates that:

a. the processor shall act only on instructions from the controller,
b. all the security obligations addressing the data controller should also be incumbent to the data processor.[58]

---

53 Again, the provision is silent as to whether the 'significant distress' should be judged subjectively or objectively.
54 Cf.Jay, P., Hamilton, A., 2003.
55 Article 17(1) data protection directive
56 Article 17(1) data protection directive
57 Cf. Siougle, E. S., Zorkadis, V.C, 2002, p. 107.

In the specific field of electronic communications, the ePrivacy directive places similar obligations on the provider of electronic communications services: he must take 'appropriate technical and organisational measures'[59] to safeguard the security of his services, if necessary in conjunction with the provider of the public communications network with respect to network security. Again, having regard to the state of the art and the cost of their implementation, these measures should ensure a level of security appropriate to the risk presented. In addition, the second paragraph of article 4 of the ePrivacy directive obliges the providers of an electronic communications service to inform the subscribers in the event of a particular risk of a breach of the security of the network (a virus or a network malfunction which could lead to data leak). The information should cover not only the nature of the risk but also any possible remedies, including an indication of the likely costs involved, in case the risk lies out of the scope of the measures to be taken by the service provider.

Finally, the data protection directive ensures that the data subject is granted with a **right to seek legal relief** to protect his privacy rights. For this purpose article 22 of the data protection directive reads: 'Without prejudice to any administrative remedy for which provisions may be made, *inter alia* before the [national Data Protection] supervisory authority, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question.' In addition, the aforementioned directive also regulates the liability of the data controller, in cases where the data subject (or indeed, 'any person'[60]) has suffered damage as a result of an unlawful processing operation or an act incompatible with the national provisions adopted pursuant to it. In such a case, the plaintiff is entitled to receive compensation from the controller for the damage suffered, unless the latter can prove that he is not responsible for the event giving rise to the damage.

A common element in many legislative texts that grant specific rights to individuals is the fact that these laws acknowledge situations in which the interests of society taken as a whole require that an individual's rights are subjugated to broader requirements. The data protection directive includes such a restraining legislative imperative in article 13, where it provides that:

"Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in articles 6 (1) [data protection principles], 10 [right of information], 11 (1) [right of information in secondary acquisition of data], 12 [right of access] and 21 [publicizing of processing operations] when such a restriction constitutes a necessary measures to safeguard:

(a) national security

(b) defence

(c) public security

(d) the prevention investigation detection and prosecution of criminal offences, or of breaches of ethics for regulated professions

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters

---

58 Article 17(3) data protection directive
59 Article 4(1) ePrivacy directive
60 Article 23 data protection directive

(f) a monitoring, inspection or regulatory function connected, even occasionally with the exercise of official authority in cases referred to in (c), (d) and (e)

(g) the protection of the data subject or of the rights and freedoms of others."

This approach mirrors the approach of ECHR which provides in respect of most of its articles that derogations are permitted where these are 'in accordance with the law' and are considered 'necessary in a democratic society'[61].

4.3 Consent

As already mentioned, personal data may be processed[62] if the data subject "has unambiguously given his consent"[63]. While this provision is the most common basis for processing data in the electronic communications sector, it presents interesting particularities when it comes to mobility. The data subject's consent shall mean 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"[64]. This definition explicitly rules out consent being given as part of accepting the general terms and conditions for the electronic communications service offered[65].

It is very important for the companies to interpret correctly the aforementioned legal provision in order to avoid violations of the data protection legislation and mainly to examine what *freely given, specific and informed* means. A *freely given* consent should not be counterpart of an advantage or subject of negotiations on behalf of the data controller. The consent needs to be *specific*, meaning that it should be given for a specific and identified scope. Finally, it needs to be *informed*; the user shall get the appropriate and sufficient information before the collection of the data and such information shall be in clear language and of course in a language that the data subject understands. A highly debated issue is whether consent can be expressed in an opt-in or in an opt-out way. It is necessary that "there must be some form of communication whereby the individual knowingly indicates consent"[66]. This can be expressed by ticking a box[67], or sending an e-mail or subscribing to a service[68].

For the processing of sensitive data the data subject shall give his *explicit* consent, although Member States may prohibit the processing of sensitive data, even with the consent of the data subject. Such legislation is very important to be known and respected. The French Data Protection Authority (CNIL) published for instance a recommendation on websites dedicated

---

[61] Article 8 European Convention on Human Rights
[62] For all the reasons that make the processing of personal data legitimate cf. Royer, D., 2006
[63] Art. 7 (a) data protection directive
[64] Art. 2 lit.h data protection directive
[65] 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. More analysis on this specific issue and specifically on unsolicited communications see Article 29 – Data Protection Working Party in its Opinion No 5/2004 on unsolicited communications for direct marketing purposes under Article 13 of Directive 2002/58/EC, adopted on 27 February 2004 (WP 90), available online at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp90_en.pdf
[66] Cf. UK Information commissioner, 2004, p. 5.
[67] Recital 17 ePrivacy Directive
[68] Cf. UK Information commissioner, May 2004, p. 5.

to health care matters[69] pronouncing among others that "health care data related to an identified or identifiable person may not be bought or sold, even if individuals to whom these data refer have given their consent"[70].

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.[71] However the aforementioned providers may process traffic data for the purpose of marketing electronic communications services or for the provision of value added services, if the subscriber or user to whom the data relate has given his prior consent[72]. A highly debated issue is how the prior given consent can be expressed. 'Some form of communication whereby the individual knowingly indicates consent'[73] (opt-in) is essential.

The sending of unsolicited communications for the purposes of direct marketing using automatic calling machines, faxes or electronic mail for the purposes of direct marketing is broadly used by companies. However this is only allowed in respect of subscribers (and not users) who have given their prior consent[74]. Although the rule for sending unsolicited communications is the acquisition of the prior consent of the data subject, Art. 13(2) data protection directive provides for an exception in the case of existing customers. According to this exception, when a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, it may use these electronic contact details for *direct marketing of its own similar products or services* provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use (opt-out).[75]

How the similarity between products and services can be defined is a matter of interpretation, differentiating between the Member States. Furthermore an issue closely related to mobility is whether a mobile communications provider is allowed to send SMS to his pre-existing customers for *direct marketing of his own similar products or services.* The ePrivacy directive mentions in Art. 13 (2) that a natural or legal person can only use the customer's 'electronic contact details for electronic mail' to send e-mails for the aforementioned purposes. Any other form of personalised marketing techniques, such as personalised mobile marketing and advertisement services shall fall outside the scope of this article. Therefore a mobile communications provider shall not be allowed to send SMS to his pre-existing customers for *direct marketing of his own similar products or services*.

---

[69] Délibération n° 01-011 du 08 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au publics, available online at http://www.cnil.fr/index.php?id=1362&delib%5Buid%5D=18&cHash=44cdf7f920 (accessed on 25 June 2008)
[70] Cf. Kuner, C., 2003, p. 71.
[71] 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*.
[72] Art. 6 (3) ePrivacy directive
[73] Cf. UK Information commissioner, 2004, p. 5.
[74] Art. 13 (1) ePrivacy directive
[75] Art. 13 (2) ePrivacy directive

4.4 Location Based Services[76]

Besides the general provisions regulating consent in relation to data protection, the ePrivacy directive includes a specific provision regarding value-added services based on location data, i.e. Location Based Services (LBS)[77]. Location data other than traffic data[78] of the user or the subscriber may only be processed when they are made anonymous. Otherwise the user or the subscriber needs to give his *consent* before the processing of location data, after being informed about the terms of such processing and the possibility to withdraw his consent for the processing of location data other than traffic data at any time [79]. According to an Opinion of the Article 29 Working Party on the use of location data with a view to providing value-added services, 'the subject of location data to be processed needs to be informed about the identity of the controller (and/or of his representative), 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 and the right to rectify the data, the right of users or subscribers 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 and the right to cancel the data'[80]. In case a service requires the automatic location of an individual, the user shall be given full information in advance about the processing of their location data and calling the relevant number shall amount to consenting to being located.[81]
The information shall be provided by the party collecting the location data for processing and thus 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 such 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. by telephoning a dedicated number)[82]. In addition, in cases of ongoing processing of location data the individual shall be regularly reminded about the processing of his location data.

A closer look to this article reveals a problem of interpretation regarding the consent of the data subject within the context of LBS. Ambiguousness arises with regard to the actual person whose consent is needed. When the user and the subscriber is the same person then the situation is clear. In electronic communications though it is rather common that one person is the subscriber and another one is the user of a device. In this case special attention should be drawn to the relation between these two. Usually, the person to whom the location data relate shall be the one who gives his consent[83]. In the example of enterprise services the employer is

---

[76] On LBS, cf. Deuker, A. (ed.), 2008.
[77] The specific provisions of the directive apply when the controller of the data is established in the European Union (Art. 3 ePrivacy dir and Art. 4 data protection directive). When the controller (provider of the value added service) is not established in a Member State, the location data may be transferred only according to the specific legislation on transfer of personal data to third countries (Chapter IV data protection directive).
[78] That is, data not used for the conveyance or the billing of the communication.
[79] Art. 9 ePrivacy Directive
[80] 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, available online at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf
[81] *Idem*, p. 6
[82] *Idem*, p. 5
[83] *Idem*, p. 6

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 employee (user).

A different situation is the purchase of an end user device by a parent for his under-aged child. Usually parents do so as an easy way to be able to track their children[84]. Most possibly the answer to our question will be different from the one given in the example of the enterprise services. In the general framework of the protection of minors, the *subscriber*, who is in this case the parent or guardian, and not the user, shall be the one to give his consent, taking into consideration the national legislation regarding the age of the minors.

4.5 Data retention

4.5.1 Why data retention?

The retention of traffic and location data is a vigorously debated issue within the European Union and has significant implications on the industry. In the frame of the European Union a 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 and amending Directive 2002/58/EC (hereinafter 'data retention directive')[85] is recently adopted. Setting aside the fierce comments against the Directive, we will restrain ourselves in examining its substantial provisions that have impact on the industry.

An issue that could lead to legal uncertainty is the lack of definition of providers that fall under 'providers of publicly available electronic communications services or of public communications networks' (Art. 1 data retention directive) for the scope of this directive. The use of these general terms creates an uncertainty as to how the Member States will define this term. Such providers can be not only telecom operators and Internet Service Providers, but also internet cafes, universities that offer use of the internet to their students or even hotels who offer the use of communication facilities to their guests[86]. An example of how much the obligation for retention of data can affect especially the SMEs in the Italian legislation that obliges internet cafes to ask for identification (keep a copy of the document) and log the user's name and the type of the identification document.

---

[84] The market is already striving to resolve this problem regarding the protection of minors. 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). 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 a new issue may come up regarding the drawing of the line between freedom of the child and parental control.

[85] 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, pp. 54–63 (March 15, 2006).

[86] Cf. Morisson, Foerster, 2006.

4.5.2 Traffic data vs. content data

The data retention directive provides for the retention of traffic and location data as well as any related data necessary to identify the user or the subscriber. However the definition of traffic data[87] is so broad that can reveal private and important information with regard to the user or the subscriber of the specific service. In the case of e-mail, as explained in detail in Working Part 29 Doc 37 'Privacy on the internet'[88], traffic data consists partly of information supplied by the sender and partly of technical information generated automatically during the processing of the e-mail. An example of traffic data are the e-mail addresses of the sender and the recipient. When the e-mail address has for instance the form 'name.lastname@law.kuleuven.be', it reveals obviously that there is a connection between the two participants in this communication, who are easily recognisable, and the collection and connection of more data might reveal personal information.

Pursuant to the goals of the new regulatory framework for electronic communications that wishes to separate the regulation of transmission from the regulation of content[89], the data retention directive does not cover data related to the content of the information communicated (content data) safeguarding the confidentiality of communications. The data retention directive does not call for the retention of traffic data related to the web browsing activities of the user. However such an obligation can be imposed by the national legislation of the Member States by virtue of Art. 15(1) ePrivacy directive which allows the retention of data for public order purposes. Therefore it is important to discuss on a 'hidden' privacy threat. The distinction between traffic data and content data is however not always as clear as the European institutions would like to believe, especially when it comes to the Internet[90]. The following example will demonstrate how traffic data can reveal simultaneously generated content data as well, unveiling personal information about the user. When the user visits a search engine, his IP address is treated as traffic data. The same happens most commonly with the URL of the requested search. If for example the user gives Google the command to look for 'scuba diving', the URL:

*www.google.com/search?hl=en&lr=&q=**scuba+diving**&btnG=Search (emphasis added)*

will be generated, an information that is automatically logged together with the time and the IP of the user. When the URL that results from a search request is combined with the IP address of the user, the aforementioned information turns into an information 'relating to an identified of identifiable natural person' and thus to personal data. The aforementioned example is only one of the cases where the border between content and traffic data is vague.

4.5.3 Types of data to be retained and retention period

The data retention directive includes a detailed list with the categories of data to be retained in Art. 5 and the main categories read as follows:

---

[87] '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" (Art. 2 (b) ePrivacy directive).

[88] Article 29 – Data Protection Working Party, 'Privacy on the Internet' - An integrated EU Approach to On-line Data Protection, adopted on 21 November 2000., 5063/00/EN/FINAL (WP 37), available at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf

[89] Recital 5 Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal L 108 pp. 33- 50 (April 24, 2002)

[90] Cf. Goemans, C., Dumortier, J., 2003.

a) Data necessary to trace and identify the source of a communication;

b) Data necessary to identify the destination of a communication;

c) Data necessary to identify the date, time and duration of a communication;

d) Data necessary to identify the type of communication;

e) Data necessary to identify users' communication equipment or what purports to be their equipment;

f) Data necessary to identify the location of mobile equipment.

The providers of publicly available electronic communications services or of public communications networks need to be very carefully about the types of data they need to retain. For instance the data retention directive stipulates that with regard to data necessary to identify the date, time and duration of a communication concerning Internet e-mail, the data that shall be retained are 'the date and time of the log-in and log-off of the Internet e-mail service, based on a certain time zone'[91] and not the time when an e-mail was sent and received.

The data retention directive provides for retention periods of not less than 6 months and for a maximum of two years from the day of the communication. Art. 15 (3) of the directive allows the Member States to postpone the application of the directive 'to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail' until 36 months after the data of adoption of the directive. 11 countries have declared to postpone the retention of such data[92].

The fact that the data retention directive does not take the modalities of Internet data into consideration is highly criticised. The volume of Internet data created every year is huge and several problems arise from these vast numbers of data that need to be retained. Furthermore the providers of publicly available electronic communications services or of a public communications network are obliged to retain all internet data for a long period of time, even when these data are never going to be useful for law enforcement purposes, like in the case of spam, which does not reveal any connection between the sender and the recipient. Moreover they need enormous storage capacities not only to save, but also to manage these data and the actual possibility to find some data that can be useful for law enforcement purposes is most unlikely. In addition to that the typical internaut leaves a 'trail', creating traffic data that can reveal much more information about his/hers habits and interests than data on whom a person was contacted by telephone.[93]

The data retention directive allows the Member States to extend the maximum retention period, when facing particular circumstances[94]. The taking of this measure shall follow an

---

[91] Art. 5. (1)(c)(2)(ii) data retention directive

[92] Council of the European Union, Declaration by delegations pursuant to Article 15(3) of the proposal for a directive, Council doc. 5777/06 ADD2 (February 10, 2006), available online at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad02.en06.pdf

[93] Commission Staff Working Document '*Annex to the:* Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC *EXTENDED IMPACT ASSESSMENT*' available at http://www.statewatch.org/news/2005/oct/com-dataret-reg-ass-05.pdf (21 September 2005), pp. 13-14

[94] Art. 12 data retention directive

immediate notification to the Commission and information to the other Member States of the measures taken, indicating the grounds for introducing them. Within six months the Commission shall approve or reject the imposed national measures. In case the Member States decide to extend the retention period for a longer period of time the economic burden on the providers of publicly available electronic communications services or of a public communications network is going to be heavy.

4.5.4 Cost reimbursement

The data retention directive does not provide for the reimbursement of the providers of publicly available electronic communication services or of a public communication network for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of the data retention directive. However, the European Commission has recognised the opinion that 'reimbursement by Member States of demonstrated additional costs incurred by undertakings for the sole purpose of complying with requirements imposed by national measures implementing this Directive for the purposes as set out in the Directive may be necessary'[95]. Although such a reimbursement could thus be granted as a legitimate state aid, the Member States are not obliged by the data retention directive to reimburse such costs[96].

4.6 Data transfer to third countries

A large amount of personal data (especially traffic and location data) is collected and processed with regard to mobility. As far as the transfer of data is realised within the Internal Market of the EU, Article 1(2) lifts the barriers between the Member States: "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1"[97]. However, in cases where the personal data are to be transferred to countries outside the European Union or the EEA, this may only take place if the third country in question ensures an adequate level of protection or if the data transfer falls under one of the statutory exceptions foreseen in Article 26 of the data protection directive. The adequate level of protection shall be acknowledged to a third country in the light of all the circumstances surrounding a (or a set of) data transfer operation(s). Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[98] With regard to transfers of personal data to third countries and further defining of

---

[95] Council of Europe, Statements, Council doc. 5777/06 ADD 1 (10 February 2006) available online at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf

[96] Problems have already arisen in Czech Republic, where the police authorities don't reimburse the telecommunications companies within a small period of time, causing huge financial problems especially to SMEs. For more information see http://www.edri.org/edrigram/number4.3/czechdataretention (accessed 16 February 2006).

97 1(1) of the data protection directive states: 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their to privacy with respect to the processing of personal data'

98 Art. 25(2) data protection directive

the notion of 'adequate level of protection' the Working Party 29 has adopted several Working Documents on the Transfers of personal data to third countries.[99]

As regards the derogations from the rule of 'adequate data protection', Article 26(1) of the data protection directive provides that a Member State may authorise a transfer of personal data to third countries which do not ensure an adequate level of protection, on one of the following conditions:

a. when the data subject has given his consent unambiguously to the proposed transfer
b. if it is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request
c. when the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party
d. if it is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims
e. when the transfer is necessary in order to protect the vital interests of the data subject
f. when the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

In addition, data transfer to third countries which do not ensure an adequate level of protection can be realised in cases where '[…] the [data] controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses'[100].

In order to facilitate the national supervisory authorities the European Commission adopted on 15 June 2001 a decision on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC)[101]. In its decision, the Commission provides the Member States with safeguards in the form of a set of standard contractual clauses. The transfer to a third country may take place, if the 'data exporter' (the controller who transfers the personal data) and the 'data importer' (the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of the decision 2001/497/EC) agree that the further processing of the personal data received by the data importer will be in accordance with the terms of the clauses.

---

99 Article 29 – Data Protection Working Party, 'Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', adopted on 24 July 1998 (WP 12), available online at: http://www.europa.eu.int/comm/justice_home/ fsj/privacy/docs/wpdocs/1998/wp12_en.pdf and Article 29 – Data Protection Working Paper, 'Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers', adopted on 03 June 2003 (WP74), available online at: http://www.europa.eu.int/comm/ justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

100 Article 26(2), Data Protection Directive

101 http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf (unter der url nicht verfügbar)

On the basis of Article 25(6) data protection directive the Commission has the power to determine whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. Until now the Commission has issued decisions[102] on the adequacy of the data protection in Argentina, Canada, Switzerland, United States - Transfer of Air Passenger Name Record (PNR) Data, United States - Safe Harbour[103], Guernsey and the Isle of Man.

Mobility creates uncertainty regarding the physical location of the processor, the controller or even the data itself. For instance an issue that generated long discussions was whether the loading of personal data on a webpage, which is accessed by some user from a country outside the EU or the EEA shall be considered as transfer of data to a third country. The Dutch Data Protection Authority stated that 'making information available through the Internet by means of a website is a form of publication'[104].

This vigorously disputed issue was resolved by the European Court of Justice, which ruled that data available on a website are not directly transferred between the person that uploaded the data and the person that accessed them but through a computer.[105] Furthermore, the Court held that '[i]f Article 25 of Directive 95/46 were interpreted to mean that there is transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. […] Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet'[106]. The Court concluded that 'there is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country'[107].

4.7 Business Compliance to European Data Protection Legislation

The data protection directive aims to provide a working balance between the needs of the data subjects and those of the data controllers by facilitating and encouraging the free flow of personal data while at the same time strictly safeguarding the privacy of the individual. Within this perspective, we can perceive data protection as a technical term relating to specific information management practices, or as the preferred stance of those who would see data protection primarily as an aspect of business regulation. In contrast, privacy is more likely to be considered as a fundamental human right and accorded specific protection under

---

102 For detailed information see:
http://www.europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm

103 The Safe Harbour Principles issued by the U.S. Department of Commerce on 21.07.2001 and the accompanying Frequent Asked Questions set forth the provisions ensuring the adequate level of data protection. For further information see http://www.export.gov/safeharbor/

104 A.D. Blas, D., Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act (WBP) Dutch Data Protection Authority, (February 2003), available online at: http://www.dutchdpa.nl/documenten/en_int_policy_paper.shtml?refer=true (accessed on 12 February 2006)

105 Judgment of the European Court of Justice (6 November 2003), Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping, par. 69

106 *Idem*

107 *Idem*, par. 71

human rights conventions or constitutions. It is however possible to discuss privacy issues in the terminology of risk and risk assessment, concepts which are, perhaps, more familiar in a business environment. In particular, three risk factors can be identified which could be considered to be elements of privacy:

a. risk of injustice: this can occur due to a significant inaccuracy in personal data, unjust inference, 'function creep' (the gradual use of data for purposes other than those for which it was collected) or reversal of the presumption of innocence as seen in data mining when correlation of information from disparate sources may produce an impression that is greater (or different) than the sum of the parts.[108]

b. risk of excessive and unjustified surveillance: the data controller could exert dubious control over the collection of personal information as a result collecting data without the data subject's consent. This risk could even extend to the active discouragement of the means to remedy these risks, such as the use of encryption and anonymising software or hardware.

c. risk to data subject's dignity: this can occur as a result of exposure or embarrassment due to an absence of transparency in information procedures, physical intrusion into private spaces, unnecessary identification or absence of anonymity, or unnecessary or unjustified disclosure of information without consent. [109]

All of the above have echoes of data protection issues and, in the technical sense, data protection measures may be considered as risk management devices which need to balance the risk to the individual from unnecessary invasion of privacy with the measures necessary to control that risk.[110]

A brief taxonomy of the various compliance costs that have an impact on the business sector must precede any analysis on the specific issues relating to the concept of mobility. These costs, as indicated by the Final Report on the Economic Evaluation of the Data Protection Directive[111] fall under the following categories:

a. costs linked to learning about the requirement of the Directive
b. costs in adjusting the internal organisation to comply with the Directive
c. running cost of compliance
d. quantity and costs of human resources involved in the compliance
e. cost of external advice and support

In addition, the aforementioned costs can be divided into three categories: Financial costs, subjective compliance costs and administrative burdens.

Financial costs are the result of a concrete and direct obligation to transfer a sum of money to the government or the competent Data Protection Authority.[112] This would include for example the one-off fee for notification that can be imposed on data controllers by the national Data Protection Authority, under article 18 of the data protection directive.

---

108 Cf., Rowland, D., Macdonald, E., 2005, p. 303.
109 *Idem*, p. 303
110 Cf. Raab, C. 1993, pp. 89-103.
111 Final Report: Economic Evaluation of the Data Protection Directive 95/46/EC (May 2005), Commissioned by the European Commission and prepared by RAMBOLL Management, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf
112 *Idem*, p. 11.

Subjective compliance costs cover expenses that businesses must undergo in order to comply with specific substantive obligations that legislation and regulation require. The investment in new technological measures in order to ensure the protection of personal data is a typical example of these costs.

Finally, administrative burdens cover the costs of business compliance with the information obligations resulting from legislation. The requirement to notify the national Data Protection Authority, for example, would fall under this category

From a different perspective, compliance costs can fall in two categories: one-off costs cover expenses and activities such as the gathering of knowledge about the requirements of the data protection directive, the initial training of the staff which by later handle the data processing, the initial notification to the competent national authority, the investment in new technology in order to ensure the secure environment in which data will be processed, etc. On the other hand, running costs include the notification to the competent authorities regarding the processing operations, the authorisation and notification of transfer of data to third countries, the training of staff in order handle new processing techniques, etc., as well as the handling of data subjects' requests for information, correction, etc. (being a legitimate exercise of their data protection rights).

In order to comply with the data protection principles laid down in the data protection directive, data controllers should store only a bare minimum of data, which suffice for the running of their services. By adopting a 'data avoidance policy'[113](that is, by implementing an infrastructure which is oriented towards collecting, processing and using either no personal data or as little as possible) data controllers can greatly minimise their compliance costs. For this purpose, it is advised that privacy issues and in particular the processing of personal data (with the further implications regarding identity management) be taken into account at the earliest stage of the organisation of the data controllers' infrastructure ('privacy by design'[114]).

Besides the use of anonymity as a weapon for compliance to data protection legislation, anonymity can also be perceived as a tool which is available to a data subject in order to shield his identity from those with whom he interacts. Current interest in this topic has primarily focused on anonymity in the context of the Internet, and the need to balance privacy through anonymity against the needs of society to be able to identify individuals engaged in particular activities. However, to the extent that electronic communication networks are converging by offering the same types of services, the relevant issues that have already emerged on the Internet are bound to occur to other electronic communications networks as well.

More specifically, a feature of all electronic communications networks is their potential to generate a huge quantity of traffic data, that is, data processed for the purpose of the conveyance of a communication on an electronic communication network or for the billing thereof.[115] The possibilities for interactive use of the networks increase the amount of traffic data yet further. It follows that the choices of the user of the network create a 'clickstream' of traffic data, which can be perceived as a 'digital trace', the monitoring of which enables the profiling of the user's online behaviour. For these reasons, the specific data also fall under the

[113] Cf. Holznagel, B., Sonntag, M., 2003.
[114] Cf. Dumortier, J., Goemans, C., 2004, p.193.
[115] Article 2 (c) ePrivacy directive.

protective scope of the legislative framework of data protection: Traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission or necessary for billing purposes. However, this obligation to erase or anonymise the traffic data does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.[116]

Moreover, the processing of traffic data by the provider of publicly available electronic communications services for the marketing of electronic communications services or for the provision of value added services may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communication services about the types of further processing it intends to perform and about the subscriber's right to give or to withdraw his consent to such processing[117]. Especially in the area of digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user fall under the definition of traffic data and therefore are regulated by article 6 of the ePrivacy directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as those providing individualised traffic information and guidance to drivers. The processing of such data for value added services should be allowed, only in cases where the subscribers have given their consent[118]. Even in these cases however, the subscribers should have simple means to temporarily deny the processing of location data, free of charge.

From a more general perspective, in order to tackle the various privacy and data protection issues that arise in respect of mobile users in a – more or less – ubiquitous computing infrastructure, businesses need to adopt a privacy driven security and data protection model, which respects and protects the privacy of the user/data subject, e.g. the user's identity and his preferences, the management of his profile. One way to develop such a privacy model is to rely on virtual identities and zero-knowledge authentication, which severs the link between the identity of the principal and the requested action.[119] A virtual identity provides anonymity to the users, which in turn calls for an implementation of a security model that ensures the accountability for potential abusers of the network. A viable solution would be the adoption of a trust-based security architecture, in which autonomous entities establish trust in other entities based on collected evidence such as reputation, recommendation and records of past experience (see, example the reputation system adopted by eBay).[120]

However, business compliance to data protection legislation should not be perceived as a passive behaviour, but as a field where initiatives to protect the privacy of the data subject are welcomed and endorsed. For example, in order to help the individuals to control the flow of the personal information when they interact in a networked environment, a new 'breed' of technologies, so-called Privacy-Enhancing Technologies (or PETs[121]) have been developed

[116] Recital 28 ePrivacy directive
[117] Recital 26 Article 6 ePrivacy directive
[118] Article 9 ePrivacy directive
[119] Cf. Farrell, S. *et al.*, 2004, p.111.
[120] Cf. Cahill, V., *et al.* 2003, pp. 52-61.
[121] Privacy-Enhancing Technologies can be defined as a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal

over the last couple of years. Their purpose is to restore the balance of power between the individual who wants to retain privacy and many other actors in the online environment who want to gather personal data. Rather than relying on the state or some industry association to deal with the possible privacy threats on a collective level, these technologies are designed to support action which confers protection only to the interested individual. It is a more realistic approach that recognises that electronic communications have massively increased scope of surveillance and thus the development of a solution is aimed to remedy the situation on the same technological level: a technological remedy for a technological threat. For these reasons and based on the 'data avoidance' principle, data controllers who are active in the field of electronic communications services should encourage their customers to use these technologies on a personal level. After all, minimising the personal data that traverse the network minimises the liability risk for the data controller in case of a breach in the security infrastructure.

data, all without losing the functionality of the information system, source: http://www.birds-eye.net/definition/p/pet-privacy_enhancing_technology.shtml

5 Theories for User Acceptance in the Market of Mobile Identity Management[122]

5.1 Introduction

Looking at the market environment, several players could be identified in the mobile market. Among others, device manufacturers, infrastructure manufacturers, network operators, mobile virtual network operators, service providers, content providers, and customers can be listed, all of whom play a major role in the process of value creation in this market. Furthermore, these players can be put into value chains, which are suitable for illustrating value-adding activities among the individual players. An example for a value chain for the mobile business market, integrating the players listed before, was suggested by Picot and Neuburger and is visualised in the following figure:

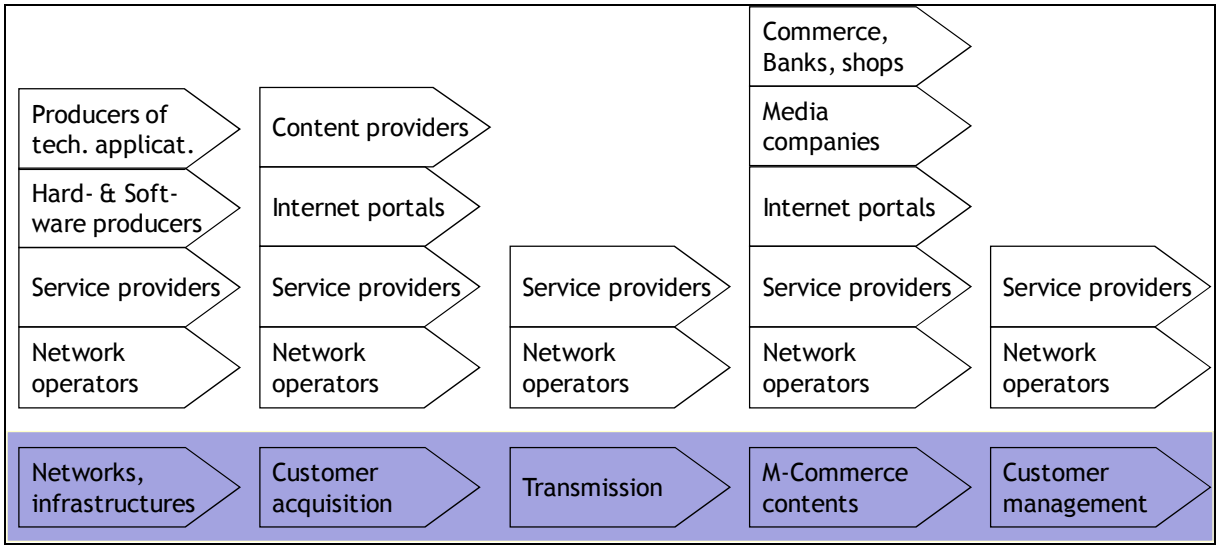

Figure 3: Mobile Value Creation: The Mobile Value Chain[123]

For the analysis undertaken here, the focus will be put on a limited number of players, resulting in a simplified value chain. The players involved here include the (1.) *mobile operator*, (2.) *the service provider* (e.g. for LBS applications and services) and (3.) *the users/customers*.[124] This is due to the following reasons:

- In this context it can be assumed that these players have the highest impact on the trust building and a possible (non-) adoption of a newly introduced service from a customer's point of view.
- The mobile operator and the service providers are the players, who are (directly/indirectly) involved with the customers/users. Accordingly, it can be

[122] Contributed by: Denis Royer and André Deuker (both JWG, Germany).
[123] Cf. Picot and Neuburger, 2002.
[124] Cf. Deuker, A. (ed.), 2008.

assumed that they have an interest in understanding the mechanisms that lead to trust building (see Chapter 5.2) and the adoption of their services (see Chapter 5.3).

To this regard, this chapter discusses the mechanisms in the market of mobile applications, the use of MIdM technology and the relevant economic theories from the customers' point of view. This should help to better understand the adoption and trust building mechanisms of customers using such mobile services (e.g. friend finder applications[125]), in order to better understand the customers' choices for *using/not using* mobile applications and services. To this regard, attitudes and behavioural elements are important aspects to explain the acceptance of technologies, such as mobile services using MIdM technology (cf. Figure 4). The relevant theories in this field are:

- Theory of Reasoned Action (TRA) → (Chapter 5.3.1)
- Technology Acceptance Model (TAM) → (Chapter 5.3.2)
- Diffusion of Innovations (DoI) → (Chapter 5.3.3)
- Price of Convenience (PoC) → (Chapter 5.3.4)

Resulting from this understanding of the relevant mechanisms, the opportunity is offered to better tailor such services to the actual needs of the targeted group.[126]

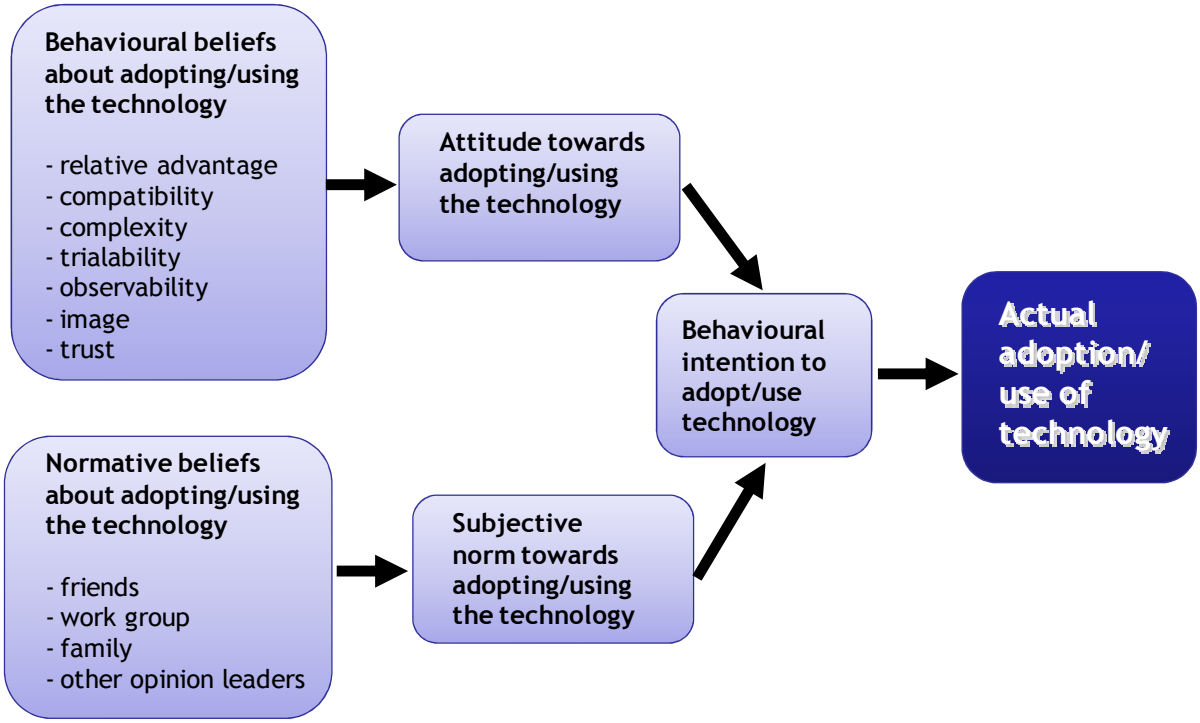

Figure 4: General Model of Technology Acceptance[127]

[125] For more scenarios, please refer to Deuker, A. (ed.), 2008.
[126] Cf. Nohria, N., Leestma, M., 2001.

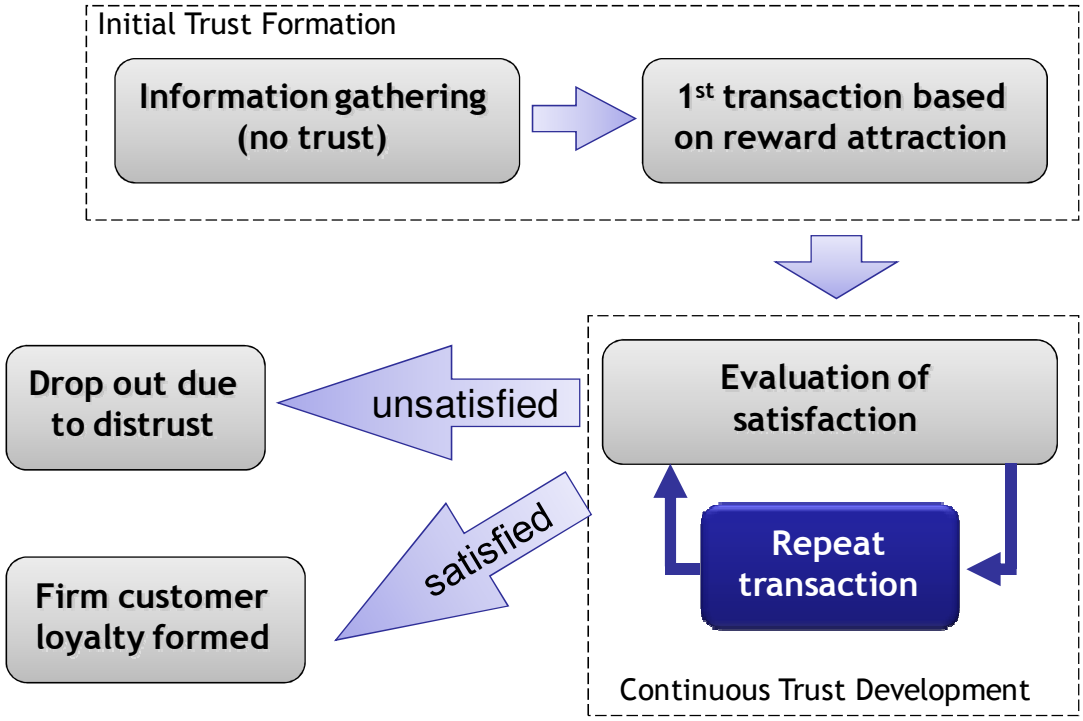

Figure 5: Schematics of the trust development life cycle[128]

5.2 Mechanisms for building User Trust

Among the many influencing factors for the usage of MIdM technologies, trust and the building of trust relationships between the different stakeholders, such as customers or service providers, can be seen as one of the most important and essential constructs. According to Boon and Holmes, trust can be defined as:

> "Trust*: A state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk"*[129]

Looking at this definition, three general characteristics of trust are highlighted:

1. A trust relationship involves two parties, namely the *trustor* and the *trustee.*
2. Trust involves uncertainty and risk.
3. The trustor has faith in the trustee's honesty and believes the trustee will not betray him.

While it is possible to identify the characteristics and the players for trust, the process of trust building towards a service or a product is important as well. One of the models to explain this process is described by Fung and Lee. Their model analyses trust building with regard to the market for mobile commerce applications (cf. Figure 5). In the opinion of the authors, this model can also be applied and extended to the domain of mobility and identity and mobile identity management. As initially stated, this is due to the fact that trust is necessary to attract users to adopt a new technology or a service.[130] Moreover, the scope of this model can be

[127] Cf. Barnes, S.J., Huff, S.L., 2003.
[128] Cf. Fung, R., Lee, M, 1999.
[129] Cf. Boon, S., Holmes, J., 1991.
[130] For the topic of adoption, please refer to Chapter 5.3.3.: "Diffusion of Innovations (DoI)".

broadened to general organisations, as not only commercial companies can offer MIdM facilities in their services and products (cp. Chapter 3.4).

According to Siau and Shen getting a potential customer to start a transaction with a service provider is the key step for initiating the trust development life cycle (cf. Figure 5).[131] In order to do this, there are various ways, such as:

- Through reward attraction, or
- By demonstrating features such as
    - convenience,
    - cost efficiency, and
    - personal necessity

Besides the general concept of trust and the trust building life cycle, the general components of customer trust need to be taken into consideration. According to Siau and Shen, the technology and the service provider are the key components, since they are considered to have the biggest impact on the customer trust. Besides these 2 factors, reliability and security of mobile technology are equally important, since failures in the early stages of the usage of M-Commerce reduce the customers' trust significantly. Moreover, as mobile technology evolves, the trust focus shifts from technology to the mobile service provider.

From a service provider's perspective, there are several steps, which need to be taken into consideration to build an initial trust formation. Among other factors, this includes the dissemination of relevant information or the cultivation of interest. Other specific ways for organisations include the following steps:

- ***Enhance customer familiarity***, as people tend to trust the familiar, e.g. by general publicity or advertisements.
- ***Build vendor reputation***, as a good reputation suggests certainty and less risk in conducting business.
- ***Deliver high-quality information***, as the information posted on a company has a high impact on the customers' perception.
- ***Elicit third-party recognition and certification***, as the independent nature of third-party certification helps customers to feel more secure in doing business with the M-Commerce provider.
- ***Provide attractive rewards***, such as free trials or gift cards helping to attract new customers.

It is important to maintain a trust relationship, as creating trust is time-consuming and trust can easily be destroyed. Accordingly, there are several successful methods derived from E-Commerce that can be adopted by organisations offering mobile services bundled with IdM functionality to overcome trust barriers. This includes the following suggestions that can be pursued by organisations to successfully overcome trust barriers:

[131] Cf. Siau, K., Shen, Z, 2003.

- ***Improve site quality:*** User-friendly design of web-sites accessed by mobile devices (e.g. giving customers sufficient information for purchases) helps to convey the vendor's competence.
- ***Sharpen business competence***: Refers to the skills, technical knowledge, and expertise in operating M-Commerce applications.
- ***Maintain company integrity:*** Providers need to be congruent with regard to the actions and the promises given to their customers.
- ***Post privacy policy:*** Similar to E-Commerce providers, M-Commerce providers should post their privacy policy online, so customers are informed about the information being processed. This helps to build transparency.
- ***Strengthen security controls:*** In order to have secure M-Commerce transactions, technologies need to be in place that help to allow Multilateral Security for all involved parties.
- ***Foster a Virtual Community:*** By building virtual communities, mobile service providers can replicate the success of web-based online communities and create positive evaluations by their users.
- ***Encourage communication and increase accessibility:*** In order to build synergies, the users should be brought into close communication with the M-Commerce provider, reducing information asymmetries and fostering the provider's credibility and trustworthiness.
- ***Use external auditing to monitor operations:*** External auditing helps to maintain the customers' trust by keeping the provider to behave fair and legally.

Figure 6 summarises the activities for initial trust building and the continuous trust development for service providers and mobile technologies into a trust building framework.

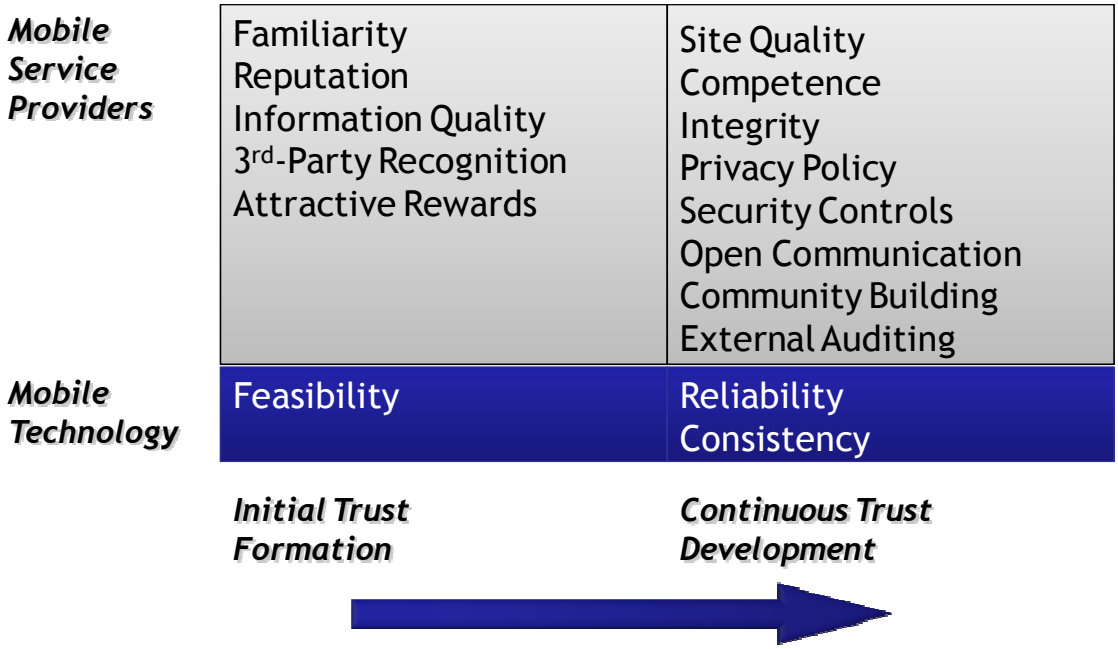

Figure 6: Derived trust building framework[132]

5.3 Theoretical foundations: Description of the Economic Theories

The following sections are dedicated towards the economic theories being used to explain the behaviour of customers and adoption mechanisms in markets. The theories being discussed are presented in the order of their appearance in the scientific literature. This is done to show their theoretical relations and links.

5.3.1 Theory of Reasoned Action (TRA)

The theory of reasoned action (TRA), developed by Martin Fishbein and Icek Ajzen, posits that individual behaviour is driven by behavioural intentions[133]. The theory received particular attention in the field of consumer behaviour as it provides a simple tool to identify possibilities to change customers' behaviour when using an innovation.[134] To this regard, the actual use of an innovation is determined by the individual's behavioural intention to use it. The model resulting from their research is visualised in Figure 7 and consist of the following components:

Starting from the *behavioural intentions*, these include the functions of an individual's attitude towards the behaviour and the subjective norm surrounding the performance of the behaviour. Accordingly, the actual use of an innovation is determined by the individual's behavioural intention to use it. The *Attitude towards an act or a behaviour* are the individual's positive or negative feelings about performing a behaviour, determined through an assessment of one's beliefs. Subjective norm is defined as an individual's perception of whether people important to the individual think the behaviours should be performed.[135] *"To put the*

[132] Cf. Siau, K., Shen, Z, 2003.
[133] Cf. Ajzen, I., 1980; Fischbein, M., Ajzen, I., 1975.
[134] Cf. Sheppard *et al.*, 1988, p. 325.
[135] Cf. Ajzen, I., 1980; Barnes, S.J., Huff, S.L., 2003.

definition into simple terms: a person's volitional (voluntary) behaviour is predicted by his/her attitude toward that behaviour and how he/she thinks other people would view them if they performed the behaviour. A person's attitude, combined with subjective norms, forms his/her behavioral intention".[136]

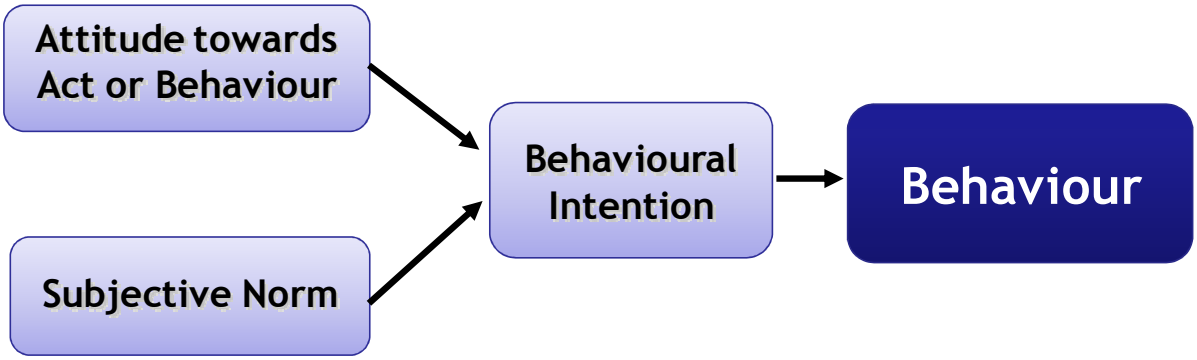

Figure 7: Schematics of the theory of reasoned action (TRA)[137]

However, the TRA has some limitations on explaining all mechanisms of the actual use of an innovation and the role of the individual's behavioural intent, which are discussed in the relevant scientific literature.[138] One limitation is the significant risk of confounding between attitudes and norms since attitudes can often be reframed as norms and vice versa. Furthermore, the assumption that when someone forms an intention to act, they will be free to act without limitation, is often unfounded. Lastly, in practice, constraints such as limited ability, time, environmental or organisational limits, and unconscious habits will limit the freedom to act.

Consequently, extended theories were needed to better describe the mechanisms that actually explain the use of an innovation and the role of the individual's behavioural intent. A selection of these theories is described in the following sections.

5.3.2 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) by Davis[139] is based on TRA and tailored towards the acceptance of information technology (IT).[140] A key purpose of TAM is to provide a basis for tracing the impact of external variables on internal beliefs, attitudes and intentions. The resulting hypothesis framework of Davis is visualised in Figure 8. In his research, two main factors are of prime relevance in explaining system usage. Namely these are:

- *"Perceived ease of use"*: The degree to which a person believes that using a particular system would be free from effort.
- *"Perceived usefulness"*: The degree to which a person believes that using a particular system would enhance his or her job performance.

---

[136] Cf. Schneberger, S., Wade, M. (eds.), 2008.
[137] Cf. Fischbein, M., Ajzen, I., 1975.
[138] Cf. Ajzen, I., 1980; Barnes, S.J., Huff, S.L., 2003; Schneberger, S., Wade, M. (eds.), 2008.
[139] Cf. Davis, F.D., 1989.
[140] In the original research by Davis, these IT systems were email systems used in an organisation.

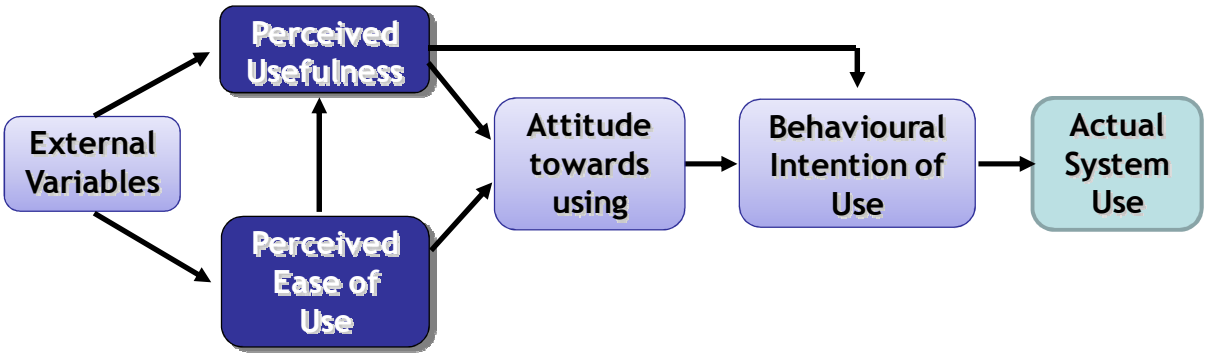

Figure 8: Hypothesis Framework of the Technology Acceptance Model (TAM)[141]

Various researchers have simplified TAM by removing the attitude construct found in TRA from the current specification (e.g. Venkatesh *et al.*).[142] Moreover, there are several attempts to extend TAM (cf. Figure 4), which generally have taken one of three approaches:

1. Introducing factors from related models
2. Introducing additional or alternative belief factors (risk, emotion, etc.)
3. Examining antecedents and moderators of perceived usefulness and perceived ease of use

Also when TAM extends TRA, some limitations can also be found:

- Both TRA and TAM have strong behavioural elements, assuming that when someone forms an intention to act, they will be free to act without limitation.
- However, in practice constraints such as limited ability, time, environmental or organisational limits, and unconscious habits will limit the freedom to act.[143]

5.3.3 Diffusion of Innovations (DoI)

The theory of the "Diffusion of Innovations" (DoI) is based on the research of Everett M. Rogers described in his 1962 book *"Diffusion of Innovations"*.[144] The theory itself describes the process by which an innovation is communicated through certain channels over time among the members of a social System. In other words, the study of the diffusion of innovation is the study of *how*, *why*, and *at what rate* new ideas and technology spread through cultures. To this regard, the theory of Rogers is an excellent resource to develop strategies in order to enable the diffusion of complex and controversial technologies in society.[145]

Adoption is similar to diffusion, except that it deals with the psychological processes an individual goes through, rather than an aggregate market process, which is described by the process of diffusion.

---

[141] Cf. Davis, F.D., 1989.
[142] Cf. Venkatesh *et al.*, 2003.
[143] Cf. Schneberger, S., Wade, M. (eds.), 2008.
[144] Cf. Rogers, E. M., 2003.
[145] Cf. Beyers, H., 2002, p. 552.

The DoI theory especially focuses on the following core topics, which will be described in the following sections:

- Adopters
- Key innovation characteristics
- Stages of adoption

5.3.3.1 Adopters

In his research, Rogers proposed that adopters of any new innovation or idea could be categorised as innovators (2.5%), early adopters (13.5%), early majority (34%), late majority (34%) and laggards (16%). Looking at the two extremes of the described groups, *"early adopters"* tend to adopt new innovations very fast, as they embrace change and are usually educated in the relevant field of the innovation being looked at. On the other hand, the adoption group of the *"laggards"* will adapt very late, as they tend to be resistant to change. Using the market for mobile services as an example, the early adopters tend to be educated, technology accepting people, who can afford to use such newly introduced mobile services. Furthermore, this group has the ability to understand the complexity of mobile services and their value added, even thought the level of uncertainty of the success of an innovation could be quite high (higher risk propensity). For the group of laggards however, this is ultimately turned to the opposite. The characteristics for the remaining adopter groups can be found in the following table:

▪ ***Innovators (2.5%):***
• ***Characteristics:*** Venturesome, educated, multiple info sources, greater propensity to take risk • Has the ability to understand and apply complex technical knowledge and can cope with a high level of uncertainty of an innovation. • The innovator is a catalyst who brings about the use and adoption of new ideas.
▪ ***Early adopters (13.5%):***
• ***Characteristics:*** Social leaders, popular, educated • Other members of the group look to these individuals for advice and knowledge about the innovation.
▪ ***Early majority (34.0%):***
• ***Characteristics:*** Deliberate, many informal social contacts • Tend to adopt the innovation just prior to time the average individual adopts it (link between early adopters and later majority).
▪ ***Late majority (34.0)%:***
• ***Characteristics:*** Sceptical, traditional, lower socio-economic status • Acceptance comes after the average person accepts
▪ ***Laggards (16.0%):***
• ***Characteristics:*** Neighbours and friends are main info sources, fear of debt • Laggards are those who are consistent or even adamant in resistance to change.

Table 1: Characteristics of adopter groups

Moreover, the adopter groups can be placed into a bell curve (cf. Figure 9 and Figure 10 for details) based on standard deviations from the mean of the normal curve, provided a common language for innovation researchers. Each adopter's willingness and ability to adopt an innovation would depend on their awareness, interest, evaluation, trial, and adoption (cf. Chapter 5.3.3.3). People could therefore fall into different categories for different innovations.

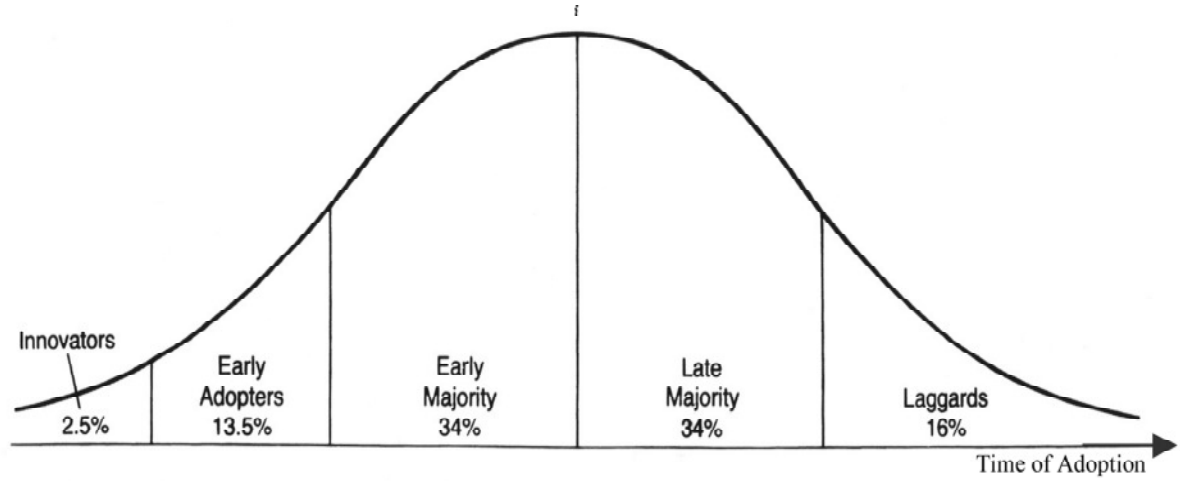

Figure 9: Adopters Bell curve

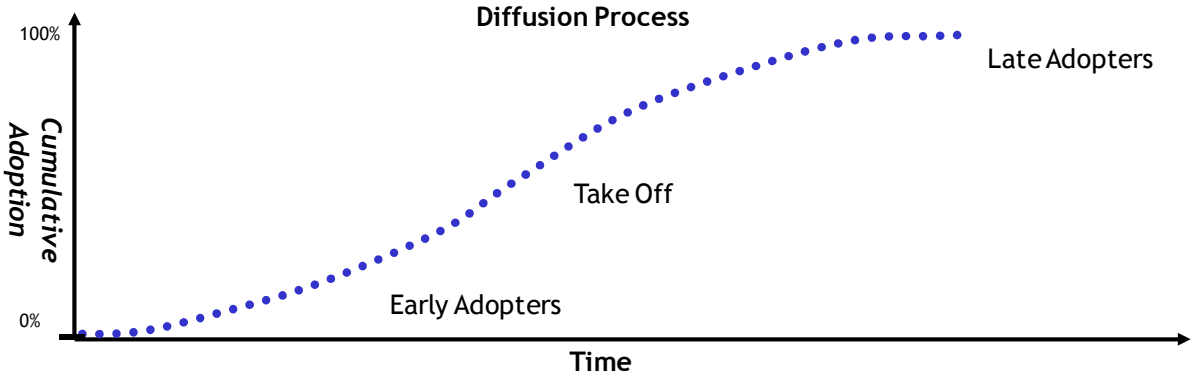

Figure 10: Cumulative adoption of an innovation over time, resulting in the S-shaped adoption curve

As a real life example for the cumulative adoption of an innovation over time, the growth of the Internet is analysed in Figure 11:

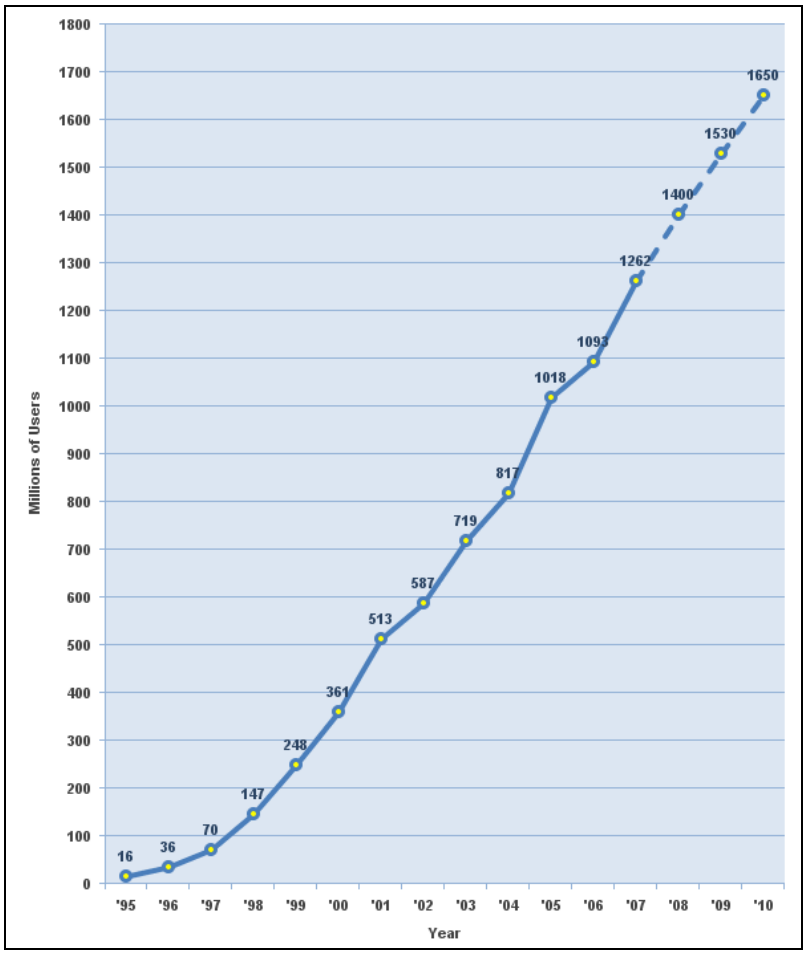

Figure 11: Cumulated growth Internet users in the world 1995-2010[146]

5.3.3.2 Key Innovation Characteristics

For the adoption itself, certain characteristics can be observed:

- ***Relative Advantage:*** The degree to which the innovation is perceived as being better than the practice it supersedes
- ***Compatibility:*** The extent to which adopting the innovation is compatible with what people do
- ***Complexity:*** The degree to which an innovation is perceived as relatively difficult to understand and use
- ***Trialability:*** The degree to which an innovation may be experimented with on a limited basis before making an adoption (or rejection) decision
- ***Observability:*** The degree to which the results of an innovation are visible to others

Following, the presented innovation characteristics are applied to the case of mobile telecommunications and its behaviour to adoption:

- ***Relative Advantage:***

[146] Please refer to http://www.internetworldstats.com for details.

- Availability/reachability of the subscriber
- Communicate (almost) anywhere / anytime
- Personal device(s)

- ***Compatibility:***
  - High compatibility in society, as flexibility and reachability become more important.
- ***Complexity:***
  - Low to medium:
    - Basic functionality (e.g. telephony) can be used by everyone being capable of using a standard, fixed-line telephone.
    - Advanced features (e.g. SMS) need further training to use them.
- ***Trialability:***
  - High: A potential customer can subscribe to a prepaid contract for testing the technology and later on switch to a "normal" subscription based contract.
- ***Observability:***
  - Reachability of the customers anytime and anywhere.
  - More and more people are using mobile phones and services.
  - People using mobile phones can easily be observed by non-users.
  - The concept and benefit of mobile telephony is easily observable by non-users.

5.3.3.3 Stages of the Adoption Process

The adoption of an innovation can be separated into the following stages:

1. ***Knowledge (Awareness):*** Learning about the existence and function of the innovation
2. ***Persuasion (Interest):*** Becoming convinced of the value of the innovation
3. ***Decision (Evaluation):*** Committing to the adoption of the innovation
4. ***Implementation (Trial):*** Putting it to use
5. ***Confirmation (Adoption):*** The ultimate acceptance (or rejection) of the innovation

In the *knowledge* stage "the individual is exposed to the innovation but lacks complete information about it". At the *persuasion* stage "the individual becomes interested in the new idea and seeks additional information about it". At the *decision* stage the "individual mentally applies the innovation to his present and anticipated future situation, and then decides whether or not to try it". During the *implementation* stage "the individual makes full use of the innovation". At the *confirmation* stage "the individual decides to continue the full use of the innovation" or not.[147] This process is visualised in the following figure (cf. Figure 12):

[147] Cf. Rogers, E., 2003.

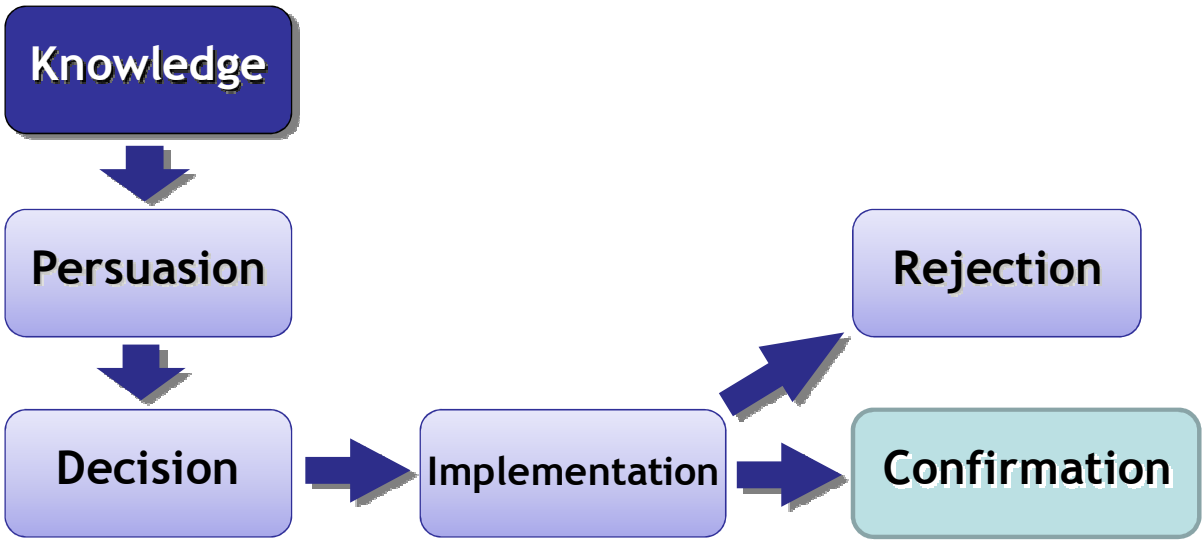

Figure 12: Diffusion of Innovations Stages of Adoption

5.3.3.4 Critique on the Diffusion of Innovation Theory[148]

Although the DoI is discussed widely in the relevant research and practitioner's literature, it also fuelled some controversy with regard to its implications and possible biases:

1. Referring to Clark and Stauton[149], the DoI theory brings in a *"pro-innovation bias"*. The DoI theory assumes that at a certain point in time, the innovations will be adopted by all members of a particular social system. As Hans Beyers[150] remarks, this bias can be seen as the result of *"[...] a historical focus of researchers towards adoption"*.[151] As a result, aspects as the ignorance and the refusal of innovations have been under exposed [152]
2. Furthermore, there seems to be an *"individual – blame bias"*.[153] This relates to the fact that people, who refuse to adopt innovations, are being reproached with it. However, one has to accept that innovations will never be perceived as useful by all people.
3. The theory of Rogers underestimates the *importance of the context* of a certain country or region. One has to keep in mind that characteristics of opinion leaders differ between different regions. Secondly the criteria to diffuse innovation and the ways of communicating and controlling communications differ also between regions.[154]

5.3.4 Price of Convenience (PoC)

Today, individuals have the possibility to interact with other people using mobile communications. To this regard, the communication between individuals and organisational bodies (cf. Chapter 3) is independent from determinants such as time and location. As mentioned before, information is the focal point, as it is provided in a non-static but

[148] Contribution by: Els Soenens (VUB, Belgium).
[149] Cf. Clarke, Stauton, 1994.
[150] Cf. Beyers, H., 2002, pp 545-570.
[151] Cf. Beyers, H., 2002, p. 558, translation by the authors.
[152] Cf. Beyers, H., 2002, p. 558.
[153] Cf. Beyers, H., 2002, p. 558.
[154] Cf. Beyers, H., 2002, p. 585.

interactive and real-time way, integrating the contextual aspects into the communication and the provision of mobile applications and services.

While an effective use of the provided data offers a higher convenience from services tailored towards the needs of users, this also can result into issues with regard to the privacy and security aspects. Consequently, the balance between convenience of service provision and security/privacy becomes an aspect to be investigated.

To this regard, the price of convenience (PoC) model was developed by Kruelle in 2002 and is based on the previously described DoI framework by Rogers.[155] The PoC model itself extends DoI, as there was a considered lack in the universal validity and incapability to capture the entire complexity of mobile technologies. To this regard, PoC can be regarded a heuristic, socio-technical tool to better understand the mechanisms customers use to trade convenience for privacy.

The *"price"* is thereby not to be understood as an economic value, but as a metaphor. The model analyses the users' willingness to trade their privacy for convenience when using mobile applications. For the cluster of MIdM, this model can help to understand how these technologies can influence the usage of mobile services in general. Also links to relevant laws and regulation in general could be analysed, as consent and a need for privacy seem to be important.

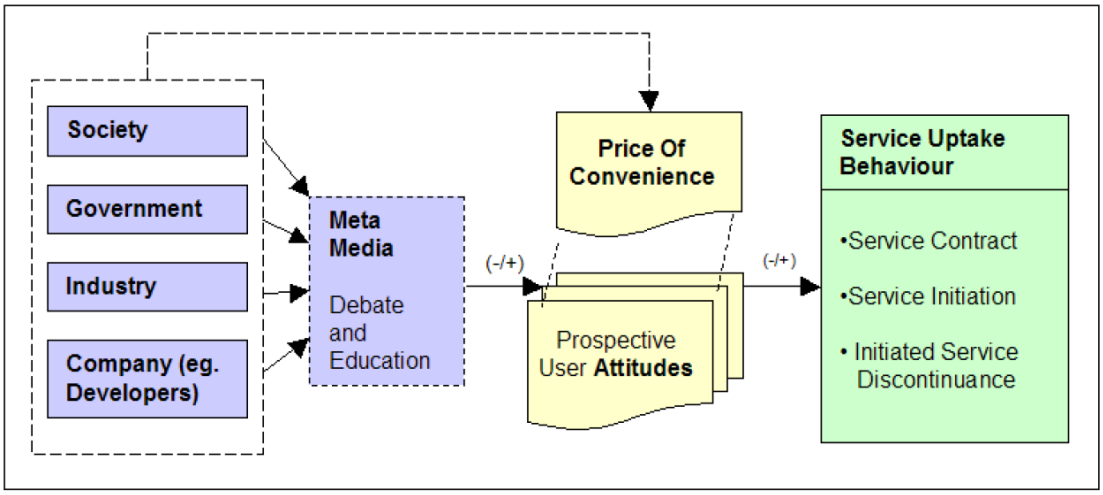

Figure 13: Conceptual framework of the "Price of Convenience" (PoC) Model[156]

As the development of innovations passes through several stages, the main influence of the PoC model can be found in the implementation and adoption phases (cf. Chapter 5.3.3.3). This separation allows the investigation of the behaviour of innovations and their development. By following this approach it is possible to identify the necessary measures to maximise the convenience. The PoC model is visualised in Figure 13 and can be further divided into the system aspects (society, government, industry, company and media) and the subjective aspects (PoC, attitudes, behaviours, and service uptake).

The decision, whether a service is adopted or not by an individual user is influenced by the individual's value towards the gained convenience and the loss of privacy resulting from a service. The derivation of the PoC is thereby significantly influenced by five discrete factors

[155] Cf. Ng-Kruelle *et al.* 2002.
[156] Cf. Ng-Kruelle *et al.* 2002; Rebne, *et al.* 2002.

recognising a diverse environment and supports both, socio-economic and technical perspectives. Namely these are: society, government, industry, companies (primary effects) and media (secondary effect), representing the *system aspects*:

- ***Society:*** For the PoC, society can be understood as a pluralistic concept in which law and order can be considered a negotiated result of different interest groups. Society is considered the strongest of the five factors
- ***Government:*** The government is considered as a monitoring entity with respect to the social security. Special emphasis is placed on the government's consideration of the protection of the individual rights' versus the *collective* safety.
- ***Industry:*** The word industry includes multiple companies offering similar products and targeting the same potential customers. Industry is credited with the capability to develop and implement standards and guidelines.
- ***Companies:*** The aspect "companies" includes developers of mobile services, technology developers, and content aggregators. From the understanding of the model, mobile service developers should especially focus on the heterogeneity of the end device in the development process, as compatibility is an important requirement.
- ***Media:*** Media are brought into the PoC model as a secondary effect, complementing the other four effects. They describe an intra-institutional setting that has a great importance for the understanding of the individual PoC as a result of influence on the privacy. Media impact is often critical for the successful adoption of a new service or product (cp. Chapter 5.3.3). Developers and mobile network operators should therefore actively approach the media to be able to influence the perception of new services.

The five presented factors influence the actual PoC, showing various interdependencies among each other. The inner attitude with regard to the adoption of a mobile application or service and the behaviour of the adopting individual are influenced by the dynamic contexts between the players in the system. As a result, the user can finally decide whether to contract, to initiate, or to discontinue a service (cf. Figure 13).

5.4 Preliminary Conclusions

As shown in the previous chapters, there are various models and theories available which help to understand the developments in the market. These models are continuously developed and extended to better explain the mechanisms behind consumer adoption and trust building.

Moreover, there are also models that are directly tailored towards the market of mobile applications and services, such as the PoC model. This is due to the fact that it has the closest relation to explain customer behaviour with regard to the trading of privacy to convenience and also links into the data protection and privacy discussion in Chapter 4. However, in order to include all relevant aspects, new and extended models seem to be necessary. Initial ideas for an approach are discussed in the following chapter.

6 Derived Framework for analysing the Economic Impacts of MIdM in Mobile Services and Applications[157]

6.1 Introduction

As shown in the previous chapters, one could identify various aspects, such as law/compliance, communicational aspects, and explanatory models that have an impact on the economics of mobility and identity and ultimately on the usage of MIdM technology in markets. All of which try to explain certain characteristics being present. However, there is no combined approach yet which includes all facets in a more holistic, explanatory framework. Based on the research by Royer and Meints[158] initial ideas for a generic explanatory framework will be proposed that will help to combine the different aspects being presented in this document.

6.2 The Balanced Scorecard Concept

During the early 1990s, Kaplan and Norton introduced the balanced scorecard (BSC) concept as a *balanced* performance measurement system for corporations, addressing shortcomings of traditional performance measurement systems.[159] In the following years, the BSC was discussed and applied in various fields.[160] Arguing that financial accounting measures, such as return on investment (ROI) or the payback period, are too narrow in their scope, the BSC does not only rely on financial outcomes.[161] To this regard it is *supplemented* with additional organisational measures that complement past and future performance indicators in a holistic way.[162]

[157] Contributed by: Denis Royer (JWG, Germany).
[158] Cf. Royer, D., Meints, M., 2008.
[159] Cf. Kaplan, R. S.,Norton, D. P., 1996.
[160] Cf. Akkermans, H. A., Oorschot, K. E., 2005; Baschin, A., Steffen, A., 2001; Martinsons, M. *et al.*, 1999; Mooraj, S.,Oyon, D. H. D., 1999.
[161] Cf. Martinsons, M. *et al.*, 1999.
[162] Cf. Kaplan, R. S., Norton, D. P., 1996; Martinsons, M. *et al.*, 1999.

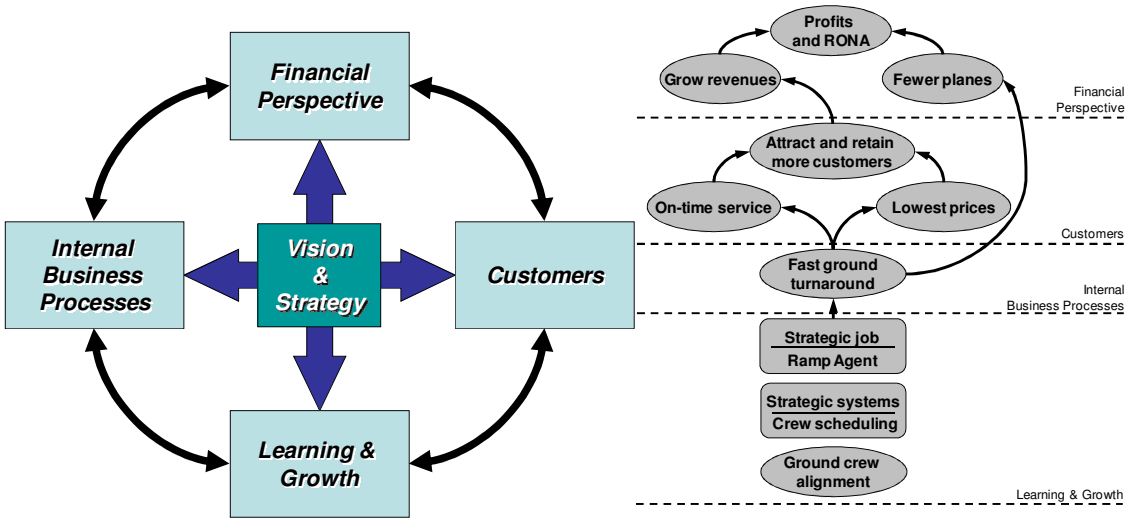

Figure 14: Examples for the balanced scorecard and strategic maps[163]

The result of Kaplan and Norton's research is a scorecard that translates additional measures into four different areas, also referred to as perspectives.[164] Namely these are: financial, customer, internal business processes, and learning and growth.[165] The resulting BSC is visualised in Figure 14. The perspectives themselves are derived from the visions and strategies of an organisation. They also represent the three major stakeholder groups of an organisation: shareholder, customers, and employees.[166]

The term *"balanced"* reflects the intent to maintain a balance between the perspectives and their contained performance indicators. Namely the balance is kept between short- and long-term objectives, lagging and leading indicators, and financial and non-financial measures.[167] Furthermore, the specific performance indicators contained in the four perspectives show interdependencies which can be further analysed by causal-chains and causal networks, also referred to as *strategic maps*.[168]

In summary, by integrating the different perspectives, the BSC allows for a more comprehensive view of the organisation itself. To this regard, the BSC strives to give a view on the historic successes and the future trends. Moreover, the BSC itself can be used to actively manage an organisation down to the project level, which helps to act in best long-term interests for an organisation.[169]

6.3 The proposed Framework for analysing the Economic Impacts of MIdM on Mobile Services and Applications

Based on the theories and aspects described in the previous chapters, the following points should be addressed, in order to derive an explanatory framework for analysing the impacts of MIdM on mobile services and applications:

[163] Cf. Kaplan, R. S. ,Norton, D. P., 1996; Kaplan, R. S. ,Norton, D. P., 2004.
[164] Cf. Akkermans, H. A., van Oorschot, K. E., 2002.
[165] Cf. Kaplan, R. S.,Norton, D. P., 1996.
[166] Cf. Mooraj, S.,Oyon, D. H. D., 1999.
[167] Cf. Akkermans, H. A., Oorschot, K. E., 2005; Martinsons, M. *et al.*, 1999; Kaplan, R. S., Norton, D. P., 1996.
[168] Cf. Jonen, A. *et al.*, 2004; Kaplan, R. S., Norton, D. P., 2004.
[169] Cf. Martinsons, M. *et al.*, 1999; Jonen, A. *et al.*, 2004.

- Derived from the theories presented before (TAM, PoC, and TRA), the driving parameters/factors for the explanation of the adoption and trust building towards a technology or a product seem to be:
    - (1.) trust,
    - (2.) perceived usefulness,
    - (3.) perceived ease of use,
    - (4.) convenience, and
    - (5.) privacy.
- Accordingly, the factors stated before should be integrated into the further analysis as parameters to be observed.
- Furthermore, by integrating the DoI, the understanding of the properties of an innovation and how the stages of the innovation's adoption process could be facilitated.
- Moreover, the players described in the simplified value chain (cf. Chapter 5.1) need to be integrated. However, the focus should be on the customer/user, as this model is built to offer the opportunity to mobile operators and service providers to streamline their product development efforts for mobile applications and to offer better products and services tailored towards the needs of users and customers.
- Accordingly, the properties and strategies towards the development of mobile applications and services are the key components to be looked at, similar to the visions and strategies presented in the original BSC.
- Finally, the aspects of law and regulation (cf. Chapter 4) should be integrated, as the impacts towards e.g. technology or society are manifold, resulting in requirements towards the safeguarding of information for mobile applications or services (cf. Chapter 4.7).

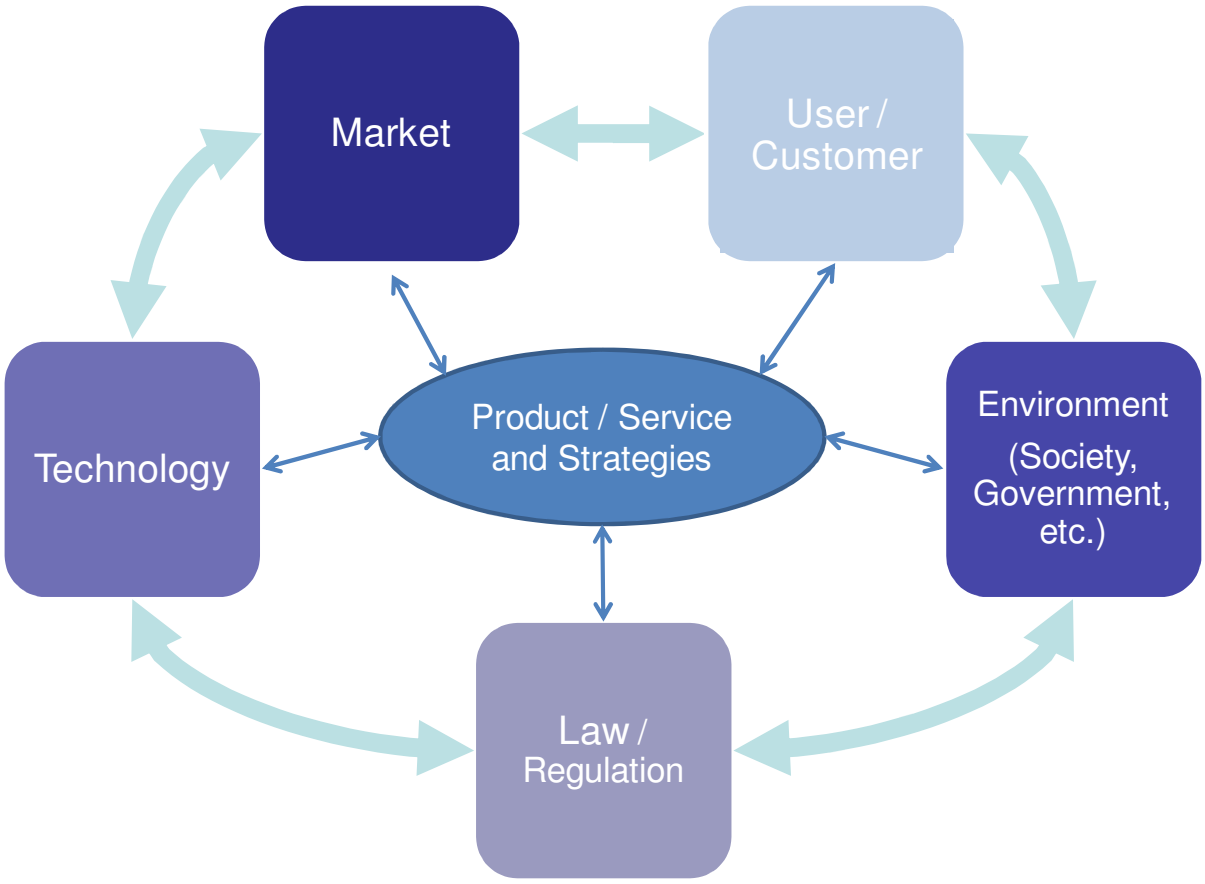

Figure 15: Perspectives of the framework for analysing the economic impacts of MIdM in mobile services and applications.

Similar to the approach taken by the BSC, the proposed framework for analysing the economic impacts of MIdM in mobile services and applications consists of five individual perspectives, which are linked to the strategies of an analysed product and service.

Namely, these perspectives are:

(1) technology perspective,

(2) market perspective,

(3) user/customer perspective,[170]

(4) environment perspective, and

(5) law/regulation perspective.

The resulting scorecard and the linkage between the perspectives is visualised in Figure 15.

For the perspectives, one could identify several quantitative and qualitative parameters and aspects that help to identify relevant properties for a product. Based on the discussions in the previous chapters, the following possible parameters could be identified:

- ***Technology perspective:*** Starting with the technology, this perspective contains quantitative and qualitative factors, such as the general properties associated to a

[170] Given the far-reaching applications and requirements one could add „citizen“ as an additional player in this perspective. However, in this analysis users and customers are in the focus, as this is an economic analysis.

technology (application field, available user base), maturity of the technology, and its ability to link to other technologies. This helps to better understand the role and linkages of a given technology, related to the other perspectives and their contained factors (e.g. the perceived usefulness or the perceived ease of use – cf. Chapter 5.3.2).

- ***Market perspective:*** In this perspectives, relevant parameters to be investigated include the observed market's structure (e.g. monopoly or polipoly), the type of market (business, private, governmental), the number of service applications or service providers, and indicators for the demand of a certain product or service. Depending on the communicational context and the actual type of market being observed, the need for privacy and security could be considered a point of reference, too (cf. Chapter 3.5).
- ***User/customer perspective:*** The user/customer perspective can be considered the most important one, as it integrates the behavioural elements, such as trust, or the willingness to adopt a certain technology (cf. Chapter 5.3.3) into the model from a user's perspective. To this regard, an integration of the user's interests would be possible, by using their individual or group preferences as the point of reference when planning mobile applications and services, in order to tailor them to their privacy or security needs. Furthermore, the critical point for the PoC, as the balance between privacy and convenience, could be identified and linked towards the technology and the environment perspective (cf. 5.3.4).
- ***Environment perspective:*** The environment perspective especially deals with qualitative factors, such as the impact of the media, the government, and society in general on the other perspectives. To this regard, environmental effects on the other perspectives can be identified, leading to a holistic view on the more intangible factors. An example could be the general opinion and discussion going on towards the usage of a technology, such as surveillance using mobile communications technology.
- ***Law/regulation perspective:*** The last perspective of the proposed framework deals with the factors resulting from business compliance, such as data protection regulation, data security (e.g. roles, access permissions), and security standards (if required). Furthermore, the regulatory needs towards the composition of a mobile application or service are contained in this perspective, such as the need for consent, purpose of used data, or the related costs to achieve these (cf. Chapter 4).

The aspects and parameters contained in the individual perspectives are not exhaustive and present a possible subset of aspects to be looked into. Also, the aspects and parameters contained in the different perspectives are not autonomous but interconnected. Further steps could include the building of causal chain models in order to identify and understand the interconnections.

Consequently, future research should extend the work presented here. This especially includes the understanding of the market reality, the application domains for the proposed framework, and the identification of relevant factors and their interconnections.

7 Conclusions[171]

Looking at the markets for mobile application and services, various players and communicational contexts can be identified as being present in the value chain for mobility and identity. As a result, mobility is becoming a major part and identities need to be managed when using mobile applications and services in order to preserve privacy and to comply with relevant data protection legislation.

Furthermore, investments in infrastructure technologies, such as MIdM in mobile applications and services are always problematic. Accordingly, one needs to understand the relevant perspectives and mechanisms that drive adoption and user trust. In this deliverable the market acceptance and the general mechanisms for the diffusion of new technologies into an emerging market were presented from various aspects.

Furthermore, an initial framework based on the balanced scorecard concept is presented. Focussing on the strategies towards the products and services the proposed framework should help to give a holistic view on MIdM technology from the relevant perspectives, as it integrates different aspects and notions. This should offer the opportunity to mobile operators and services providers to streamline their product development efforts for mobile applications and to offer better products and services tailored towards the needs of users and customers.

7.1 Outlook

Two factors show the strong relation between mobility and identity:

1. Mobility of people requires advanced identity solutions. This could be seen when the GSM Mobile Communication networks were established: A relevant part of their design are the Subscriber Identity Module (SIM) and the concept of international roaming, that allow users to be internationally mobile and to use communication services based on their business relations at home and without major organisational overhead.
2. The establishment of the GSM infrastructure has provided the mobile operators with strong instruments to manage identities. Not only are the mobile operators in a stronger position than most fixed-line telephone operators, who only know that their lines lead to a building or a household. The mobile operators are also on the verge of using identity information in other application fields, e.g. marketing and advertising.

For some future developments there are already elements visible:

1. The downturn in the revenues for pure communications drives the telecommunications industry towards new business models, adapted e.g. from the media industry: The revenue for establishing a (mobile) communications connection between two people gets smaller and smaller, so the operators need to search for income elsewhere. At the same time advertising that addresses individuals or at least people in a specific context and with a specific profile becomes worthwhile, as it seems to be promising in the fight for consumers' attention. So (mobile) telecommunication operators are moving

[171] Contributed by: Kai Rannenberg and Denis Royer (both JWG, Germany).

into the field of business matchmaking, which creates many interesting questions on their future role, e.g. as intermediary in a two-sided market: *Will this be a sustainable business? Will they have enough trust from consumers for this?*

2. The relatively strong identity technology of mobile phones and SIM (chip) cards encourages the use of the mobile infrastructure for applications, that are not directly communication related, e.g. for payment via the mobile phone or for authentication towards accounts (personal bank accounts as well as job related accounts). The fact that mobile phones have a display is of use here. So will mobile phones be the platforms for future identity related business and employee transactions? Will their technology and the mobile communication infrastructure be robust enough for sustainable security in this area?
3. The move towards electronic passports and identity cards communicating with their environment over RFID technology is confronted with a fundamental problem. A passport/ identity card that has only the RFID chip and the corresponding reader to communicate with the outer world has no effective means to check and assess the trustworthiness of the reader. Can mobile phones and SIM card be a model for the "stronger user authentication device"? Or will future passports and identity cards get their own different means of communication? What will the distribution infrastructure for identity of this type look like?

FIDIS Deliverable D11.11 "Future of Mobile Identity - Next Generation Networks and Mobile Services" will aim to answer some of these and related questions.

8 References

8.1 Bibliography

1. Ajzen, I., *Understanding Attitudes and Predicting Social Behaviour,* Prentice-Hall, Englewood Cliffs, NJ, 1980.
2. Akkermans, H. A. and Oorschot, K. E., *A Case Study of Balanced Scorecard Development Using System Dynamics, Journal of the Operational Research Society,* Vol. 56, No. 8, pp. 931–941, (2005).
3. Akkermans, H. A. and van Oorschot, K. E., *"*Developing a Balanced Scorecard with System Dynamics*"*, *Proceeding of 2002 International System Dynamics Conference,* 2002.
4. Article 29 – Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, adopted on 24 July 1998 (WP 12), available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf (accessed 25 June 2008).
5. Article 29 – Data Protection Working Party, *Privacy on the Internet - An integrated EU Approach to On-line Data Protection*, adopted on 21 November 2000, 5063/00/EN/FINAL (WP 37), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf (accessed 25 June 2008).
6. Article 29 – Data Protection Working Paper, *Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, adopted on 03 June 2003 (WP74), available online at: http://www.europa.eu.int/comm/ justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf (accessed 25 June 2008).
7. Article 29 – Data Protection Working Party, *Opinion No 5/2004 on unsolicited communications for direct marketing purposes under Article 13 of Directive 2002/58/EC*, adopted on 27 February 2004 (WP 90), available online at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp90_en.pdf (accessed on 25 June 2008).
8. 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 (accessed on 25 June 2008).
9. Baecker, D., *Organisation als System*, Suhrkamp Verlag, Frankfurt am Main 1999.
10. Barnes, S.J., Huff, S.L., *Rising Sun: iMode and the Wireless Internet*, Communications of the ACM, Vol. 46, No. 11, pp. 79-84, 2003.
11. Baschin, A. and Steffen, A., *IT-Controlling mit der Balanced Scorecard, Zeitschrift für Controlling u. Management,* Vol. 45, No. 6, pp. 367-371, (2001).
12. Bergmann, M., Rost, M., Pettersson, J. S., *Exploring the Feasability of a Spatial User Interface Paradigm for Privacy-Enhancing Technology*, in Nilsson, A. G. *et al.* (eds.),

Advances in Information Systems Development: Bridging the Gap between Academia and Industry, Springer Verlag, Heidelberg, 2005.

13. Blas, A.D., *Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act*, (WBP) Dutch Data Protection Authority, (February 2003), available online at: http://www.dutchdpa.nl/documenten/en_int_policy_paper.shtml?refer=true (accessed on 12 February 2006).
14. Beyers, H., *Het internet en de informatiesamenleving – criteria voor de adoptie van nieuwe technologie*, *tijdschrift voor sociologie,* volume 23, nr. 3-4, p 545- 570, 2002.
15. Boon, S., Holmes, J., *The dynamics of interpersonal trust: Resolving uncertainty in the face of risk*, in Hinde, R., Groebel, J. (Eds.): *Cooperation and Prosocial Behaviour,* Cambridge University Press, Cambridge, pp. 190–211, 1991.
16. Büllingen,F., Stamm, P., *Mobile Multimedia-Dienste: Deutschlands Chance im globalen Wettbewerb*, Bundesministerium für Wirtschaft und Arbeit, 2004.
17. Cahill, V., Shand, B., Grey, E., Dimmock, N., Twigg, A., Bacon, J., English, C., Wagealla, W., Terzis, S., Nixon, P., Bryce, C., di Marzo, G., Seigneur, J.M., Carbone, M., Krukow, K., Jensen, C., Chen, Y., Nielse, M., *Using Trust for Secure Collaboration in Uncertain Environments*, Pervasive Computing, July-September 2003, pp. 52-61, available at: http://www.cis.strath.ac.uk/research/publications/papers/strath_cis_publication_262.pdf (accessed on 25 June 2008).
18. Clarke, Stauton, *Innovation in technology and organization*, Londen Routledge, 1994.
19. Commission Staff Working Document, *Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC EXTENDED IMPACT ASSESSMENT*, available at http://www.statewatch.org/news/2005/oct/com-dataret-reg-ass-05.pdf (Accessed on 21 September 2005).
20. Council of Europe, *Statements*, Council doc. 5777/06 ADD 1 (10 February 2006) available online at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf (accessed on 25 June 2008).
21. Council of the European Union, *Declaration by delegations pursuant to Article 15(3) of the proposal for a directive*, Council doc. 5777/06 ADD2 (February 10, 2006), available online at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad02.en06.pdf (accessed on 25 June 2008).
22. Danezis, G., Lewis, S., Anderson, P., *How Much is Location Privacy Worth?, 2006*, available online at http://infosecon.net/workshop/pdf/location-privacy.pdf (accessed on 25 June 2008).
23. Davis, F. D., *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*, MIS Quarterly Vol. 13, No. 3, pp. 319-339, 1989.
24. Deuker, A. (ed.), *FIDIS Deliverable D11.2 "Location Based Services"*, Frankfurt a. M. 2008.

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, L 281, 23.11.1995, p. 0031-0050.
26. Directive 97/66/EC of the European Parliament and the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector, O.J. L 53, 14 January 1998.
27. Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal L 108 pp. 33- 50 (April 24, 2002).
28. 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.
29. 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 and amending Directive 2002/58/EC. Final text of the directive (not yet published in the Official Journal) cf. Council doc. 3677/05 (February 03, 2006) available online at http://register.consilium.eu.int/pdf/en/05/st03/st03677.en05.pdf (accessed on 25 June 2008).
30. Dumortier, J., Goemans, C., *Privacy Protection and Identity Management*, in Blažič, B., Schneider, W., Klobučar, T. (eds.), *Security and Privacy in Advanced Networking Technologies*, Ios Press, 2004, pp. 191-212.
31. Farrell, S., Seigneur, J.M., Jensen, C., *Security in Exotic Wireless Networks*, in Blažič-Jerman, B., Schneider, W, Klobučar, T., (eds.), *Security and Privacy in Advanced Networking Technologies*, IOS Press, 2004, pp. 101-114.
32. *Final Report: Economic Evaluation of the Data Protection Directive 95/46/EC* (May 2005), Commissioned by the European Commission and prepared by RAMBOLL Management, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf (Accessed on 25 June 2008).
33. Fishbein, M., Ajzen, I., *Belief, attitude, intention, and behavior : An introduction to theory and research*, Don Mills, Ontario: Addison-Wesley, Reading (Mass.) USA, 1975.
34. Fung, R., Lee, M., *EC-Trust (Trust in electronic commerce): Exploring the antecedent factors*. In Proceedings of America Conference of Information System, 1999.
35. Garfinkel, S., Rosenberg, B. (eds.), *RFID Application,* Security, and Privacy, pp. 189-200, Addison-Wesley, New York 2005.
36. Gasson, M., Meints, M., Warwick, K. (eds.), *FIDIS Deliverable D3.2 "A Study on PKI and Biometrics"*, pp. 41-47, Frankfurt a. M. 2005.
37. Goemans C., Dumortier J., *Enforcement Issues - Mandatory retention of traffic data in the EU: possible impact on privacy and on-line anonymity*, in Nicoll, C., Prince, J.E.J., van Dellen, M.J.M (eds.), *Digital Anonymity and the Law, Information Technologies & Law Series (2)*, T.M.C. Asser Press, 2003, pp. 161-183, available online at

http://www.law.kuleuven.ac.be/icri/publications/440Retention_of_traffic_data_Dumortier_Goemans.pdf?where= (accessed on 17 October 2005).

38. Gudauskaite, S., Peciura, L., *Electronic Signature: E-Document Exchange in Lithuania's Public Sector*, *Baltic IT&T Review* (34) 2004, pp. 15-17, Vilnius 2004.
39. Hansen, M., Berlich, P., *Identity Management Systems: Gateway and Guardian for Virtual Residences*, EMTEL Conference: New Media, Technology and Everyday Life in Europe Conference, London 2003. Download see http://www.lse.ac.uk/collections/EMTEL/Conference/papers/hansen_berlich.pdf (Accessed on 25 June 2008).
40. Holznagel, B., Sonntag, M.., *A Case Study: The JANUS Project,* in Nicoll, C., Prins J.E.J., van Dellen, M.J.M. (eds.), *Digital Anonymity and the Law – Tensions and Dimensions*, TMC Asser Press, The Hague, 2003, pp. 121-135.
41. IPTS, *Security and Privacy for the Citizen in the Post September 11 Digital Age: A Prospective Overview*, 2003, available online at ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf (Accessed on 25 June 2008).
42. Jay, R., Hamilton, A., *Data Protection Law and Practice*, Sweet & Maxwell, London, 2003.
43. Jonen, A. *et al.*, *Balanced IT-Decision-Card, Ein Instrument für das Investitionscontrolling von IT-Projekten, Wirtschaftsinformatik,* Vol. 46, No. 3, pp. 196-203, (2004).
44. Judgement of the European Court of Justice, *Case C.I.L.F.I.T. v. Ministry of Health*, Case 283/81 (1982) ECR 3415.
45. Judgment of the European Court of Justice (6 November 2003), *Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping*.
46. Kaplan, R. S. and Norton, D. P., *Strategy maps,* Harvard Business School Press, 2004a.
47. Kaplan, R. S. and Norton, D. P., *The Balanced Scorecard. Translating Strategy into Action,* Random House, 1996.
48. Kieserling, A., *Kommunikation unter Anwesenden – Studien über Interaktionssysteme,* Suhrkamp Verlag, Frankfurt am Main, 2000.
49. Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, 2003.
50. Luhmann, N., *Organisation und Entscheidung*, Westdeutscher Verlag, Opladen/Wiesbaden 2000.
51. Martinsons, M., Davidson, R. and Tse, D., *The balanced scorecard: a foundation for the strategic management of information systems, Decision Support Systems,* Vol. 25, No. 1, pp. 71-88, (1999).
52. Meints, M., Hansen, M. (eds.), *FIDIS Deliverable D3.6 "A Study on ID Documents"*, pp. 41-47, Frankfurt a. M. 2005.
53. Mooraj, S. and Oyon, D. H. D., *The Balanced Scorecard: a Necessary Good or an Unnecessary Evil?, European Management Journal,* Vol. 17, No. 5, pp. 481-491, (1999).

54. Morisson, Foerster, *Data retention – Implications for Business*, February 2006, available online at http://www.mofo.com/mofo_dev/news/updates/files/update02138.html (accessed on 13 February 2006).

55. Nabeth, T., Hildebrandt, M. (eds.), *FIDIS Deliverable D2.1 "Inventory of Topics and Clusters"*, Frankfurt a. M. 2004.

56. Ngai, E. W. T. and Gunasekaran, A., A review for mobile commerce research and applications, Decision Support Systems, Vol. 43, No. 1, pp. 3-15, (2007).

57. Ng-Kruelle, G., P. Swatman, D. Rebne and F. Hampe, *The Price of Convenience: Privacy and Mobile Commerce*, Quarterly Journal of Electronic Commerce, Vol. 3, No. 3, pp 273-385, 2002.

58. Nohria, N., Leestma, M., *A moving Target: The Mobile-Commerce Customer*, MIT Sloan Management Reviews, Spring 2001.

59. Picot and Neuburger, Mobile Business – Erfolgsfaktoren und Voraussetzungen, in: Mobile Kommunikation, Reichwaldt (Hrsg.), Gabler, Wiesbaden, 2002, pp. 55-69.

60. Raab C., *The Governance of Data Protection,* in Kooiman, L. (ed.), *Modern Governance*, Sage Publications, London 1993, pp.89-103.

61. Rebne, D., G. Ng-Kruelle, P. Swatman and F. Hampe, *Weberian Socioeconomic Behavioral Analysis and Price-of-convenience Sensitivity: Implications for MCommerce and Location-based Applications*, 2002 CollECTeR (Europe) Conference on Electronic Commerce, Centre de Congres, Toulouse, France, 2002.

62. Ristola, A., Koivumaki, T., Kesti, M.: The Effect on Familiar Mobile Device and Usage Time on Creating Perceptions Towards Mobile Services, International Conference on Mobile Business (ICMB'05), pp. 384-391, 2005.

63. Rogers, E. M., *The Diffusion of Innovations*, 5th Edition, Free Press, New York, London, Toronto, Sidney, 2003.

64. Roussos, P.D., Peterson, D., Patel, U., *Identity Management; an Enacted View,* International Journal of E - Commerce, vol. 8, number 1, M.E. Sharpe Armonk NY, 2003, pp.81–100.

65. Rowland, D., Macdonald, E., *Information Technology Law*, 3rd edition, Cavendish Publishing, London 2005.

66. Royer, D. (ed.), *FIDIS Deliverable D11.1: 'Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity'*, Frankfurt, 2006

67. Schneberger, S., Wade, M. (eds.), *Theories Used in IS Research Wiki*, http://www.fsc.yorku.ca/york/istheory/wiki/index.php/Main_Page, York (Canada), 2008 (Accessed on 30 June 2008).

68. Sheppard, B. H., Hartwick, J., & Warshaw, P.R., *The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research*, Journal of Consumer Research, Vol. 15, pp. 325-343, 1988.

69. Siau, K., Shen, Z., *Building Customer Trust in Mobile Commerce*, Communications of the ACM, Vol. 46, No. 4, 2003, pp. 91-94.

70. Siougle, E.S., Zorkadis, V.C., *A Model Enabling Law Compliant Privacy Protection through the Selection and Evaluation of Appropriate Security Controls*, in Davida, G., Frankel Y., Rees O., (eds.) *Infrastructure Security*, Proceedings of InfraSec International Conference (2002, Bristol, UK), Springer, 2002, pp. 104-114.

71. 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).

72. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D., *User acceptance of information technology: Toward a unified view,* MIS Quarterly, Vol. 27, No. 3, pp. 425-478, 2003.

8.2 Hyperlinks

- http://www.cio.de/markt/800187/ (accessed on 25 June 2008).
- http://www.dafu.de/praxis/militaer.html (accessed on 25 June 2008).
- http://de.itronix-europe.com/News/News_Article.asp?id=254 (accessed on 25 June 2008).
- http://www.toughbook-europe.com/DEU/business_kompetenz.aspx (accessed on 25 June 2008).
- http://www.intergraph.com/military/mobilesolutions.asp (page not found).
- http://www.ipsi.fraunhofer.de/mobile/teaching/seminar-ws0304/BOS_Polizei.pdf (accessed on 25 June 2008).
- http://www.hessen-media.de/mm/egovernment-in-hessen-CeBIT-2004.pdf (accessed on 25 June 2008).
- http://www.hessen-egovernment.de/dynasite.cfm?dssid=72&dsmid=1957&dspaid=14090 .
- http://www.aselsan.com.tr/msting/mobKomKont_eng.htm (page not found).
- http://www.hessen-egovernment.de/dynasite.cfm?dssid=72&dsmid=1957&dspaid=14102 .
- http://www.hessen-egovernment.de/dynasite.cfm?dssid=72&dsmid=1957&dspaid=14088 .
- http://usa.autodesk.com/adsk/servlet/item?format=print&id=4621255&linkID=3514346&siteID=123112 (page not found).
- http://www.prime-project.eu.org/public/prime_products/PRIME-White-Paper-V1.pdf (page not found).
- http://www.trackyourkid.de/ (accessed on 25 June 2008).
- http://puremobile.de/index.php?cPath=21 (accessed on 25 June 2008).
- http://www.dafu.de/rechts/rechts-wap.html (accessed on 25 June 2008).
- http://www.nokia.de/de/hintergrundberichte/2002/25540-popupContentArea.html (accessed on 25 June 2008).
- http://www.wirtschaftsrat.de/data/landesverbaende/HH/Digitale_Trends11-2004.pdf (accessed on 25 June 2008).
- http://www.anon-online.de (accessed on 25 June 2008).
- http://tor.eff.org (accessed on 25 June 2008).
- http://www.signatur.rtr.at/de/providers/services/mobilkom-a1signatur.html (accessed on 25 June 2008).
- http://mobile.aol.com/portal/main.php (accessed on 25 June 2008).
- http://www.t-zones.de/de/index.html (accessed on 25 June 2008).

- http://www.egovernment-akademie.de/academy/content/sections/ (accessed on 25 June 2008).
- http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=3337 (accessed on 25 June 2008).
- http://www.kronegger.at/?url=newsletter-200502a-mobile&lang=en (accessed on 25 June 2008).
- http://www.gizmodo.com/archives/sk-telecom-human-ear-gps-kids-phone-018408.php (accessed on 25 June 2008).
- http://www.engadget.com/entry/1234000203040158 (accessed on 25 June 2008).
- http://www.engadget.com/entry/1234000550052710 (accessed on 25 June 2008).
- http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf (accessed on 25 June 2008).
- http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad02.en06.pdf (accessed on 25 June 2008).
- http://www.statewatch.org/news/2005/oct/com-dataret-reg-ass-05.pdf (accessed on 25 June 2008).
- http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf (page not found).
- http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf (page not found).
- http://www.europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm (accessed on 25 June 2008).
- http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf (accessed on 25 June 2008).
- http://www.birds-eye.net/definition/p/pet-privacy_enhancing_technology.shtml (accessed on 25 June 2008).
- http://www.internetworldstats.com (accessed on 25 June 2008).