FIDIS

Future of Identity in the Information Society

Title:	D7.7: RFID, Profiling, and AmI
Author:	WP7
Editors:	Mireille Hildebrandt (VUB), Martin Meints (ICCP)
Reviewers:	Denis Royer (JWG, Germany), Claudia Diaz (KUL COSIC)
Identifier:	D7.7
Type:	[Deliverable]
Version:	1.0
Date:	Thursday, 31 August 2006
Status:	[Final]
Class:	[Public]
File:	fidis-wp7-del7.7.RFID_Profiling_AMI.doc

Summary

The target of this study is to provide a multifocal perspective on the workings of radio frequency identification (RFID) technologies, integrating technical, social and legal perspectives. As this deliverable is part of the work package on profiling, it regards RFID as an enabling technology for Ambient Intelligence, the 'Internet of Things' or the age of 'everyware'. Ambient Intelligence (AmI) implies a real time adaptive environment in which most adaptive decisions are taken by machines in a process of machine to machine communication. These decisions are based on what is called autonomic profiling, severely restricting human intervention, while being in need of a continuous and dynamic flow of information. This raises many of issues that need to be anticipated and dealt with. This deliverable will provide a descriptive analysis to prepare the way for more fundamental research into the possibilities to integrate legal and technological solutions and more specific research into the development of a holistic privacy framework for RFID technologies. Both are taken on in the third work plan of the FIDIS NoE.

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

Copyright Notice:

Members of the FIDIS consortium

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

Versions

Version	*Date*	*Description (Editor)*
0.1	16.03.06	• Consolidated format for the deliverable, based on agreement of the D7.6 Workshop in January 2006
0.2	24.04.06	• Initial release (Mireille Hildebrandt VUB), Martin Meints (ICCP), first draft of chapters 1 and 2
0.3	26.05.06	• Integrated version with first drafts of all chapters to be reviewed by the editors
0.4	02.06.06	• Integrated version including first draft of all chapters, with editors comments, sent off to all contributors
0.5	20.06.06	• Integrated version of revised chapters + new chapter 6
0.6	07.07.06	• Edited version, including executive summary and conclusions to reviewers
0.7	28.07.06 02.08.06	• Review Claudia Diaz • Review Denis Royer
0.8	04.08.06	• Revised version integrating the comments of the reviewers • Sent round to the authors
0.9	14.08.06	• Feed-back from Bert-Jaap Koops, Sabine Delaitre, Mark Gasson and Collette Cuijpers integrated, summary on the front page integrated, glossary and bibliography finalised
1.0	30.08.06	• Final editorial finishing

Foreword

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

Chapter	*Contributor(s)*
1 Executive Summary	Mireille Hildebrandt (VUB); Martin Meints (ICPP)
2 The Link between Profiling, RFID and AmI	Martin Meints (ICPP); Mireille Hildebrandt (VUB)
3 Cases & Scenarios	Martin Meints (ICPP); Denis Royer (JWG); Sabine Delaitre (IPTS)
4 Legal Aspects	Eleni Kosta, Michaël Vanfleteren (KUL ICRI); Colette Cuijpers (TILT), Bert–Jaap Koops (TILT)
5 Social Aspects	Sabine Delaitre (IPTS); Martin Meints (ICPP); Els Soenens, Mireille Hildebrandt (VUB); Ruth Halperin (LsE)
6 Implications for Democracy and Rule of Law	Mireille Hildebrandt (VUB)
7 Conclusions	Martin Meints (ICPP), Mireille Hildebrandt (VUB)
8 Annex	Mark Gasson (Reading University), Markus Hansen (ICPP)
9 References	All authors, Els Soenens (VUB)
10 Abbreviations & Glossary	Mireille Hildebrandt, Martin Meints (VUB)

Table of Contents

1 Executive Summary

The target of this study is to provide a multifocal perspective on the workings of radio frequency identification (RFID) technologies, integrating technical, social and legal perspectives. As this deliverable is part of the work package on profiling it regards RFID as an enabling technology for Ambient Intelligence, the 'Internet of Things' or the age of 'everyware'. Ambient Intelligence (AmI) implies a real time adaptive environment in which most adaptive decisions are taken by machines in a process of machine to machine communication. These decisions are based on what is called autonomic profiling, severely restricting human intervention, while being in need of a continuous and dynamic flow of information. This raises many of issues that need to be anticipated and dealt with. This deliverable will provide a descriptive analysis to prepare the way for more fundamental research into the possibilities to integrate legal and technological solutions and more specific research into the development of a holistic framework for RFID technologies. Both are taken on in the third work plan of the FIDIS NoE.

Today's RFID tags* and related systems show a number of remarkable technical capabilities such as:

- The 'always on' nature of today's mainly used RFID tags*
- Open accessibility to large parts of RFID systems*
- The possibility to install and run RFID systems* hidden (including RFID tags*), without user's recognition and interaction
- The possibility to build up an ubiquitous reader* infrastructure combining fixed installed reader networks with mobile readers* and seamless network connection allowing real time automated data collection and processing

In this context **control** will become one of the central issues. For every implementation of RFID in this context the following aspects have to be taken into consideration:

- From the perspective of the operators
  - Liability
  - Compliance (including data protection and security safeguards for personal data)
  - IT-Security in the context of assessing business risks
  - Technology acceptance and success on the market
- From the perspective of the users social aspects including
  - Erosion of Privacy

  - Discrimination, exclusion and victimisation as consequences
  - Helplessness might lead to reactions such as technology avoidance (‘*digital refuseniks*’) or even open resistance

From the perspective of democracy and rule of law what strikes one, is the potential shift in power between the data controllers and the users, due to the knowledge profilers will develop about citizens and the inadequacy of the present legal and technological infrastructures to make transparent the construction and application of such profiles. The resulting need for a rebalancing process cannot be solved by simple enacting new laws or developing more privacy enhancing technologies (PET*). The research presented in this report demonstrates that there is no solution that is technical, legal or socio-economic only. All aspects have to be taken into account. In this way the deliverable prepares the way for D7.9 (on ambient law, which aims to integrate mandatory data protection legislation into the technological infrastructure and aims to provide smart proxies to allow citizens real-time negotiations concerning their privacy level) and D12.3 (which aims to develop a holistic model for RFID).

Suggestions for different stakeholders developed in this document are:

- *Politicians and citizens need to foster*
  - Public debate, e.g. participatory Technology Assessment
- *Social science and social theory*
  - Next to mainstream sociological research more investments need to be made in socio-technical research that looks into the nexus of human and nonhuman attachments in order to fully comprehend and anticipate the type of world that is under construction.
  - The TFI model provides a salient insight into the technological, the formal and the informal layers of the development and application of emerging technologies. Also Actor Network Theory provides an adequate framework to detect relevant developments because it refuses to pay tribute to classic distinctions between intentional actors and passive material technologies.
- *Technicians need to invest in further research and development directed towards*
  - Improved security
  - PETs* and TETs* (Transparency Enhancing Technologies)
- *Business enterprise needs to be aware that*
  - A cheap and technologically simple implementation of RFID may not be efficient due to liability, security and privacy-compliance problems.
  - Careful planning and continuous monitoring and improvements are necessary.
  - In this context appropriate trust models, taking a firm basis in the trust from the perspectives of the users, can play an important role.

- *Legislators*
  - Need to contemplate integration of legislation into the technological infrastructure to render effective e.g. the fair information principles
  - Need to face the fact that an AmI environment implies autonomous profiling, which is at odds with some of the basic tenets of data protection (data minimisation, explicit consent, right against automated decision processes)
  - Need to extend their focus on protection of personal data (data minimisation principle) to a focus on effective access to group profiles that may be applied to an individual person, even if they were inferred from anonymised data or data of other persons
  - Need to anticipate the emergence of new liability issues (both civil and criminal) and to foresee new methods of criminal investigation that may need new types of safeguards.

2 Introduction

Martin Meints (ICPP), Mireille Hildebrandt (VUB)

This document is the second of three deliverables currently (August 2006) planned in the context of RFID within the FIDIS Network of Excellence. It uses a number of terms and concepts that will not be explained in depth in this document as they will be dealt with in other FIDIS deliverable. The most important terms in the context of this deliverable we marked with a "*". These terms are shortly introduced and explained in chapter 10 (Abbreviations & Glossary).

In this chapter we start with a pointed analysis of the links between radio frequency identification (RFID), the 'Internet of Things' and (autonomic) profiling. After this an introduction is provided on how Ambient Intelligence (AmI) is related with technologies we know today, especially RFID systems* and profiling techniques. To enable the understanding of the linkage between these technologies, RFID is briefly introduced including relevant privacy and security aspects. To allow the comparison of AmI-systems with today's RFID systems* generic models for both systems are introduced.

2.1 RFID, the 'Internet of Things' and autonomic profiling

2.1.1 Introduction

From March to September 2006 the European Commission has initiated a Public Consultation on RFID and 'The Internet of Things', having invited a number of stakeholders to exchange information on the technological state of the art and to share their viewpoints on the wider implications of a tagged environment.[1] During this consultation it became clear that RFID systems* form a potent enabling technology for AmI or networked adaptive environments. Far beyond the state of the art of supply chain management, RFID-applications were for instance presented as smart solutions for critical infrastructures, e.g. flood alert systems.[2] Crucial infrastructures will profit from the fact that RFID systems* can provide an X-ray vision of presently invisible (undetectable) layers of reality.[3] This is the case because the borders between the online and the offline world begin to blur as *THINGS* go online, creating what is now called *The Internet of Things* (ITU, 2005), or, as Adam Greenfield (2006) says, creating the dawn of 'everyware'. As it was repeated during many of the presentations, the 'Internet of Things' makes devices smart, which are not necessarily smart by themselves, but smart because they are connected. These connections allow machine-to-machine (M2M) communication, leading to an environment that functions like a unified interface, producing a very different case than explicit control.[4] M2M communication in fact produces autonomic

[1] See at www.rfidconsultation.eu
[2] See the presentation of Dr. Gilles Privat, Senior Scientist, France Telecom R&D at http://www.rfidconsultation.eu/docs/ficheiros/au_conf670306_privat_en.pdf
[3] See the presentation of Dr. Frank Stajano, Lecturer, University of Cambridge, at: http://www.rfidconsultation.eu/docs/ficheiros/au_conf670306_stajano_en.pdf.
[4] See the presentation of Dr. Gilles Privat, Senior Scientist, France Telecom R&D at http://www.rfidconsultation.eu/docs/ficheiros/au_conf670306_privat_en.pdf

computing, implicating real-time monitoring and real-time decision-making without human intervention.[5] Evidently, such autonomous processes challenge our sense of privacy, control and personal autonomy. In the next section a brief analysis will be made of autonomic computing and the autonomic profiling it implies.

2.1.2 Autonomic computing and autonomic profiling

In 2001 Paul Horn, vice-president of IBM, coined the term autonomic computing. His concept basically refers to the process of interconnected processing of data, gathered from 'everyware',[6] involving continuous M2M communication and M2M decision-making. What is special about the concept of autonomic computing is the focus on the self management of the network (Kephart, Chess, 2003). The intelligence that evolves from such a network implies pro-active instead of inter-active computing: We are not asked to program our preferences, the whole idea is that we need not interfere because the 'everyware' infers our preferences even before we become aware of them. Paul Horn's choice of the term 'autonomic' was inspired by the subconscious functioning of our autonomous nervous system that is likewise pro-active and manages both our continuous adaptation to the internal and external environment and its own repairs. Autonomous computing seems to represent a shift from human to digital butlers, always unobtrusively anticipating one's need one step ahead.[7] However, to enable this butlerisation of the material environment we need a permanent data shadow,[8] infinitely sharper than human memory, never fading, presenting us with an effective denial of oblivion.[9]

Autonomic computing presumes autonomic profiling, which could be defined as a reiterative process of construction and application of profiles, entangling real time monitoring and real time M2M decision making. The adaptive environments envisioned in AmI depend on such autonomic profiling, restricting human intervention to revisions of the software. Such revision seems marginal, because autonomous computing depends on auto-revision of the software by the network itself. It may be the case that human intervention will eventually focus on the end-user who wants to introduce deliberate changes in his relationship with the adaptive environment. Most probably the end-user will need autonomic devices to reset his default positions. This could mean that the time will come that only those humans that have access to the right type of autonomic devices can interact with their environment in an autonomous way.

2.1.3 Privacy and autonomy in the age of 'everyware'

If the reader is not familiar with concepts like autonomic computing, 'everyware', etc. he may feel nauseated by the fantastic perspectives presented in this section and even take a sceptical

---

[5] See the presentation of Dr. Krishna Nathan, Director IBM Zurich Research at http://www.rfidconsultation.eu/docs/ficheiros/au_conf670306_nathan_en.pdf

[6] 'Everyware is information processing embedded in the objects and surfaces of everyday life' (Greenfield, 2006: 18).

[7] See the presentation of Dr. Frank Stajano, Lecturer, University of Cambridge, at: http://www.rfidconsultation.eu/docs/ficheiros/au_conf670306_stajano_en.pdf.

[8] A data shadow is a term used by Stajano (see previous footnote) to indicate the data we leak while moving around the Internet of Things, and which follows us like shadow. Cp terms like 'electronic footprint' that indicate the way such leaking of data allows tracing and tracking.

[9] Idem.

stand against such apparent 'belief' in the powers of technology. The point is, however, that our environment may be changing both swiftly and radically (Garreau, 2004). If these technologies take on, they may create a technological infrastructure that will impact our lives in existential ways. This is not to confess to technological determinism, but to acknowledge that technologies such as RFID systems* may come to determine fundamental aspects of our life. In section 5.3 the difference between technological determinism and different strands of constructivism will be further discussed. The awareness of the widespread social implications of a technology once it has taken its place in society is the reason why many of the presentations at the Public Consultation referred to privacy by design: We should NOT wait until the infrastructure is a *fait accompli*, but weave the technical possibilities for adequate end-user controls into the technologies as they emerge and enter the market. As many speakers remarked, data protection legislations seem hopelessly impotent as long as the technological means to implement its principles are absent. Some speakers argued for a mandatory privacy assessment of new technologies and mandatory introduction of PET* applications. At the same time the focus on individual deliberate consent, purpose limitation seems inadequate in the face of a technological infrastructure that aims to relieve us from the burden of deliberate interaction (replacing this with invisible pro-active M2M communication) and builds on total correlatability of 'everyware' (including all our data all the time everywhere). The focus on personal data instead of on electronic footprints seems to render data protection legislation outdated and ineffective as to the real threats to be faced. Both the legal and the technological infrastructure need crucial updates to recreate the adequate safeguards for constitutional democracy. In this deliverable the focus will be on a multidisciplinary description of the technological state of the art, use cases and prospective analysis, followed by an analysis of the existing legal framework and a survey of social aspects. In the new Work Package 12 on emerging technologies, especially in deliverable 12.3 a holistic framework will be elaborated to meet some of the challenges relating to RFID. In deliverables 7.8 and 7.9 the challenges of autonomic profiling will be studied in terms of the need for a closer integration of legal and technological frameworks.

2.2 Generic Understanding of AmI-Systems from a Technical Perspective

From a technical perspective, we understand AmI-systems as systems that enable:

- Ubiquitous computing* support
- Simplified human computer interactions (HCI) including advanced interfaces compared to today's keyboards and mice
- Automated adaptive environment with respect to the preferences of the users (for example concerning light, temperature, audio and visual media etc.)
- Automated execution of repeating processes such as orders of every day's products

To implement these requirements, AmI-systems need an infrastructure with the following abstracted technical components:

- Ubiquitous interfaces and sensors*
- Ubiquitous infrastructure for data transport
- Computing power and software facilitating decision making based on artificial intelligence*
- Data storage
- Interfaces to external data and services
- Components to execute decisions such as actuators etc.

As a result we can describe in a generic way AmI-systems as follows:

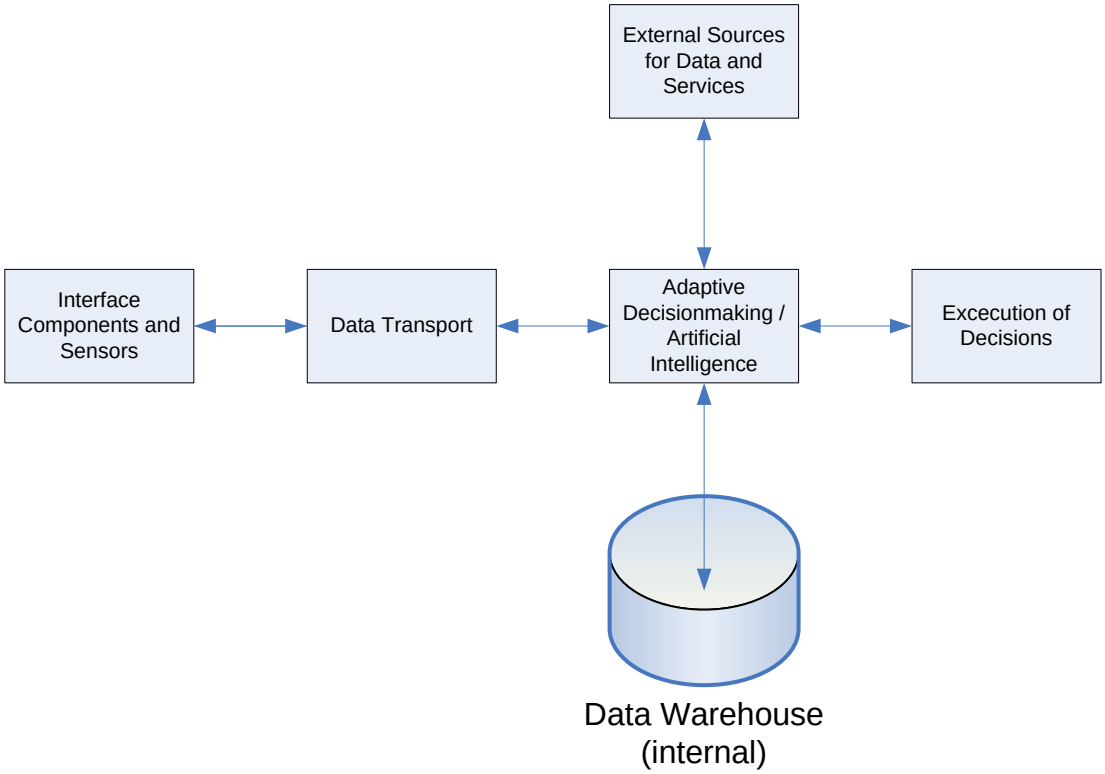

Figure 1: Generic scheme of an AmI-system

The linkage of AmI with profiling has already been analysed in the FIDIS-Deliverable D3.7 (Schreurs, Hildebrandt, Gasson, Warwick, 2005). Profiling is the central enabling technique that links data collection and processing to adaptation of the environment. It is obvious that the use of personalised profiles* for example in a smart home is a very well understood method to make decisions for adaptation. In the following sub-chapter we will look into the linkage between AmI, profiling and RFID.

2.3 RFID, RFID systems* and Identification

A brief overview on RFID tags*and readers* is given in the Annex (chapter 8) and will be further investigated and described in the FIDIS Deliverable D3.7.

RFID tags* cannot be used in a meaningful way on their own. They are always part of an RFID system* (RFID systems* are described in chapter 2.6). Possible components of RFID systems* are (Garfinkel, Rosenberg, 2005):

- RFID tags*; we understand an RFID tag* as a device that is composed of a chip storing data and / or being able to perform simple computing operations. Directly attached to this chip is an antenna for radio frequency transmission and / or the receiving of electric power (passive tags, see Annex, chapter 8.2)
- The corresponding readers*
- An infrastructure for data transport from the reader(s)* to the computing device
- Computing device and software facilitating matching and identification
- A reference database providing reference data to compare the information and /or identifier stored on the RFID tag*
- Interfaces to external data and services
- Components to use the results of the matching process for example Supply Chain management systems (SCM), Manufacturing Management systems (MM) etc.

Today RFID systems* are mostly used in supply chain management (SCM) with the target to substitute the traditional barcodes. RFID tags* for that purpose have to be very cheap (throw away electronics) and therefore are mostly simple devices in a technical sense. They are able to store and transmit one identifier only (for example an EPC*, cp. Annex, chapter 8.4.2), when empowered electromagnetically and read out by a reader* (passive RFID tags*). In this context they are mainly used to identify objects, in this case the products in the supply chain.

But today's RFID tags* do not stop to respond to readers* after the product is bought by a customer and leaves the supply chain (unless special measures to destroy or deactivate the tags are taken). In this context the link between the RFID tag* and the product and may create a link between the product and the customer. In an indirect way the RFID tag* may now be used to identify the owner / user of the product. This works very well in cases where RFID tags* are linked physically in a stable way to the product (for example in case a RFID tag* is integrated into the sole of a shoe) and where the product is not used by many users (most people don't exchange their shoes with other persons on a regular basis). But in many other cases the stability of the link between an RFID tag*, an object and a person is very questionable. This problem of the stability of the links is a problem similar to the one we observe for example with identification and determination of the location of a person using mobile phones (Royer, 2006).

RFID tags* are also used to identify persons directly and specifically or in a more generic way. Examples for this are the VeriChip[10], that can be implanted to support the identification of persons through RFID systems*, RFID to lock and unlock the doors of cars (identifying a presumably authorised user of the car), or the SpeedPass system[11] implemented by ExxonMobile, that allows for a simplified payment via a credit cards and thus identifies the user indirectly as the credit card holder.

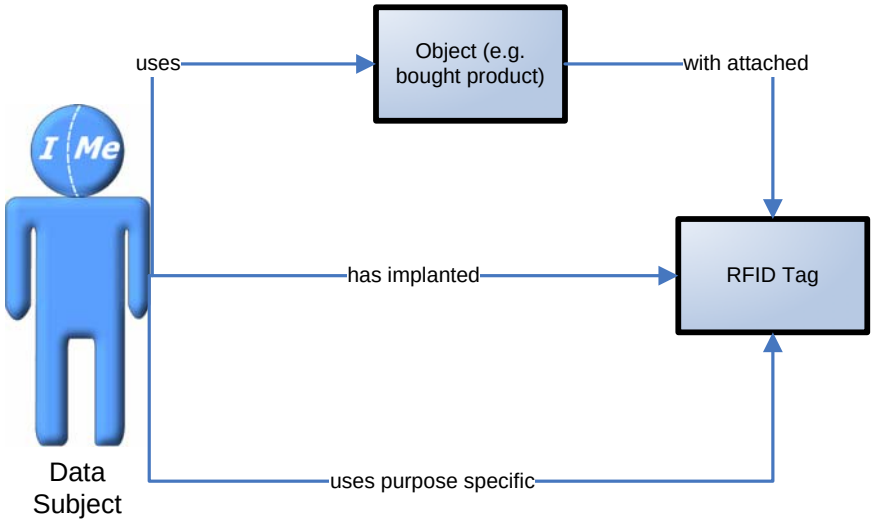

Figure 2: Examples of different kinds of links between a person and a RFID tag*

2.4 Non-interactive Authentication and Tracking using RFID

RFID tags* can be read out remotely from various distances, depending on the used radio frequencies and other physical effects (cp. Annex, chapter 8.3). In the case that a RFID tag* is linked directly (implant) or indirectly (via a product) to a person, it is probable that the person will not be able to observe that the tag has been read, who controls the reader*, how and to what purpose the data from the tag are being processed etc. Like certain types of biometrics (especially behavioural biometrics, but also face recognition; cp. Gasson, Meints Warwick (2005) for further information on Biometrics) RFID can be used for unobserved and non-interactive authentication of persons. This kind of authentication is also called 'passive authentication' in non-academic literature.[12]

From a privacy perspective unobserved and non-interactive authentication is of special interest, as this kind of authentication undermines effective exercise of the right of individuals for data self-determination. Although we know of proposed technical measures that allow for example the detection of certain types of RFID tags* and methods to log access to RFID (Floerkemeier, Schneider, Langheinrich, 2004), we do not know of any generally usable and reliable technical method to prevent unobserved and non-interactive authentication of persons

[10] See http://www.verichipcorp.com/, accessed on 29th of June 2006
[11] See https://www.speedpass.com/forms/frmSpHome.aspx, accessed on 29th of June 2006
[12] The term 'passive authentication' is ambiguous, as it is also used to describe parts of the self-testing routine of RFID tags in Machine Readable Travel Documents, see (Meints, Hansen, 2006). We therefore decided not to use this term further in this document in the context of unobserved and non-interactive authentication.

via today's RFID systems*. All known approaches, such as the Faraday cages[13] or so-called blocker tags (Juels, Rivest, Szydlo, 2003), work for known and obvious tags or specific frequencies only. In this context a digital-rights-management-like (DRM*-like) approach for data collected by any RFID reader* on the world has been discussed (Molnar, Soppera, Wagner, 2005) recently, but given the enormous problems with today's DRM*-approaches this seems neither easy to implement technically, nor easily enforceable on the market.

Rieback, Crispo and Tanenberg (2005) suggest a so called RFID Guardian. This is a PDA like device allowing for detection of tags and readers and supporting among others access management for RFID tags through external readers by acting as RFID proxy. In the context of this concept today only basic functions such as RFID tag* and reader* detection and jamming (for jamming c.p. chapter 5.1.3.2.2) are available in a prototype.[14] Most of the planned access management functions are not supported by todays mainly used RFID tags*.

Another known approach is the implementation of a cryptographic key that restricts the access to the data on an RFID tag* of the type 'microcontroller' (cp. Annex, chapter 8.2). Microcontrollers could potentially reduce or take away the need for centralised reference databases for some areas of application of RFID. But today's implementation of microcontrollers, for example in Machine Readable Travel Documents (MRTDs), show a number of severe technical and conceptual problems, such as cryptographic weaknesses and the access to the data via a - from the perspective of the bearer of the RFID tag* non-trusted – reader*. Future developments of microcontrollers certainly can improve the situation, but as microcontrollers will be much more expensive compared to today's simple tags used in SCM it is not very likely that they will substitute simple tags in the near future.

RFID today, for example, is used to track goods in the supply chain as already explained. In cases where the link between an RFID tag* and a person is stable, RFID tags* can be used to track persons as well, leading to profiles on their movement (when has she or he been where?). To facilitate this, a network of readers* with known reader* locations is needed. While some experts argue that such a ubiquitous reader* network is not very realistic, others claim that via customer loyalty programs and the corresponding data exchange of many participating shop operators, a far reaching reader* network could easily be established (Garfinkel, Rosenberg, 2005).

2.5 RFID systems*, AmI-systems and Security

Another aspect that has been an issue for debate is the security of RFID systems* when used autonomously or integrated in a larger AmI environment. The target of IT security management is to establish the required level of:

(1) Confidentiality of the (sub-) system,

(2) Availability and

(3) Integrity of the processed data in any operational phase.

The security of RFID systems* is dependant on:

[13] Definition see http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci942282,00.html, accessed on 29th of June 2006

[14] See http://www.rfidguardian.org/prototype.html, accessed on 21st of August 2006

(1) The effectiveness of technical security measures for all components of RFID systems* and

(2) The organisational security of all organisations and individuals that use the RFID system* or take part in it (knowingly, not knowingly or unobserved).

While the manipulation of databases using especially programmed RFID tags* has already been exploited (Rieback 2006), we do not know of scenarios, where a reader* manipulates already programmed RFID tags* (technical security of already issued RFID tags* seems to be sufficient with respect to this type of attack). But many other, traditional attacks directed to any other component, such as the readers* (for example denial of service) or the networking infrastructure for the data transport (for example man-in-the-middle-attacks*), have to be dealt with when building up security concepts for RFID systems* as well. Organisational measures will always be difficult to implement, as relevant parts of the RFID systems* are physically open accessible (e.g. RFID tags*, readers*, wireless networks) and effective control of the behaviour of all persons passing by will mostly be impossible. Technical security measures will become increasingly important, as they can be implemented and controlled centrally much more easily.

Another security-aspect of RFID systems* will gain increasing importance when integrating RFID systems* in AmI-systems. As those systems interconnect with supporting services and a number of technical systems behind this, these supporting systems will affect the security of the AmI- and the RFID systems* as well. It is likely that these supporting systems will be operated by different service providers, so there is no central control from the perspective of security over the AmI- and RFID system*. To establish multilateral security in interconnected systems according to ISO/EIC 27001[15], all participating parties need among others:

(1) Co-ordinated security concepts,

(2) Mutual contracts to ensure the implementation and

(3) Appropriate mutual audit schemes.

In any case, the establishment of information security in an AmI-environment using RFID systems* will be no trivial task, due to the technical and organisational complexity. This will affect professional operators of AmI-systems like in a shopping mall as well as persons operating a smart home.

2.6 The Linkage between AmI, Profiling and RFID

A number of systems known today can be understood as forerunner technologies or basic enablers for AmI. Examples are:

(1) RFID systems*,

(2) Biometric systems, and

(3) Location based services (LBS) using mobile devices.

[15] See for example the Baseline Protection Manual, which is since January 2006 part of the ISO/EIC 27001. The corresponding requirements are listed in chapter 3.10 (generic module "Outsourcing"). See http://www.bsi.de/english/gshb/manual/download/index.html, accessed on 29th of June 2006

Profiling, which enables the detection of significant patterns in the data collected by means of these technologies, can include autonomic, real time decision making that is the *conditio sine qua non* for an AmI environment. Especially RFID systems* are - from an abstracted technical perspective - very similar to future AmI-systems.[16] The similarities become obvious by comparing Figure 1 with generic RFID systems* (c.f. Figure 3):

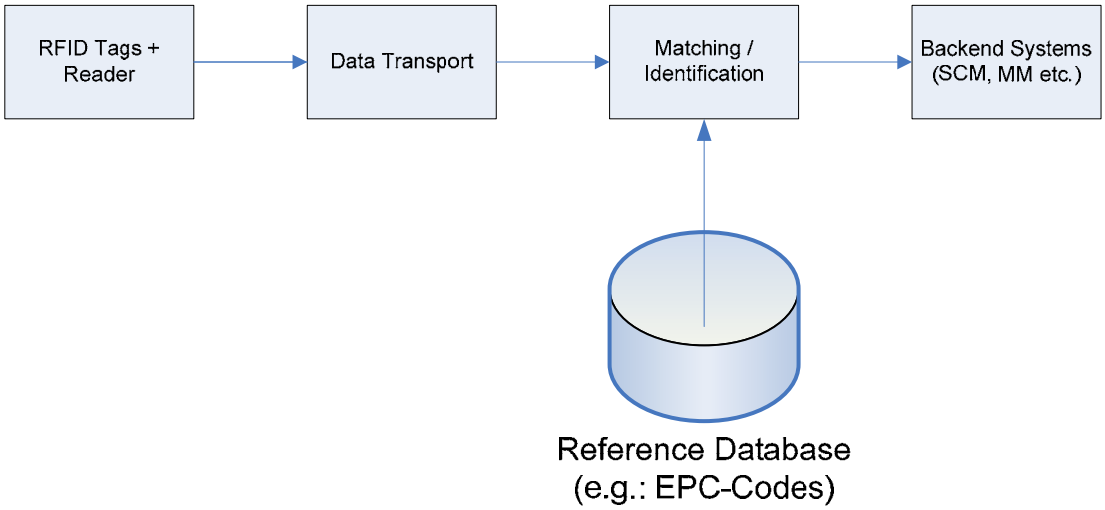

Figure 3: Scheme of a generic RFID system*

With a few modifications for example (1) by adding data mining to the matching process (could be done by installing additional software on the central computation device), (2) extending the database to a data warehouse to store additional data about performed matching processes (data from which reader* at what location? Match to what reference data?) one can use an RFID system* for profiling purposes. The objective of such profiling could be user tracking or generation of decisions for a (hidden) adaption of the environment. Especially in the latter case the resulting combined system shares many characteristics with AmI-systems, when adaption of the environment is implemented.

As the user in this case is not necessarily aware of being authenticated and does neither control the decision process, nor the adaption of the environment, from his perspective the environment is manipulated by others. Obviously the test of this kind of combined systems (RFID + profiling + adaption) has been prepared for, at least technically and legally (see the case study of the Metro Future Store, chapter 3.2).

2.7 Summary

RFID and related systems can be understood – together with other technologies - as forerunners for AmI. From this point of view we can expect that AmI-systems will share (in addition to aspects resulting from the combination of different forerunner technologies) a number of technical, legal and social characteristics from RFID systems*. As explained in

[16] See for example the Technology Guide of the Auto-ID center (2003). Download via http://interval.hu-berlin.de/downloads/rfid/technologische%20grundlagen/Technology_Guide.pdf, accessed on 29th of June 2006

section 2.1 RFID systems* can connect an 'Internet of Things' that integrates autonomic computing and autonomic profiling, changing the way we relate to our environment in a radical way. In the next chapter state-of-the-art cases and prospective scenarios will be presented to provide a better picture of what such an environment may look like.

3 Cases & Scenarios

3.1 Introduction

In this chapter a set of three case studies will be presented to provide an idea of state of the art use of RFID as an enabling technology for AmI. Section 3.2 presents a case study on the Metro Future Store, which tested the use of RFID beyond the supply chain to profile customers and provide better services; section 3.3 presents a case study on the use of RFID in the educational setting of a museum to enhance interactive communication and guidance for visitors; section 3.4 present a study on the use of RFID in a US pharmacy chain to enhance drug management and prevent mistakes.

After the cases, which deal with the state of the art, a set of three scenarios will be presented to provide some idea of the direction in which RFID applications may develop (prospective research). Section 3.5 presents a scenario for social inclusion of visually handicapped people; section 3.6 presents a scenario on security risks in the case of RFID enhanced clothes; section 3.7 presents a scenario on privacy risks in the case of RFID enhanced products in the case that profiling is used for customer relationship management (CRM).

3.2 Case study: the Metro Future Store in Rheinberg[17]

Martin Meints (ICPP)

In Rheinberg, Germany, the Metro group as the third largest retailer in the world runs the so-called “Future Store”, in which the use of RFID is being tested.[18] The testing exceeds the use of RFID tags* in the supply chain, as the tags are used directly in the shop at least with a selected number of products. Functions and services that use (or plan to use) RFID are:[19]

- Smart shelves within the store for automated positioning of products and automated orders in case a certain number of products of a certain type falls short of the predefined number
- Smart weighting machines which automatically detect the product and calculate the price
- Electronic price tags at the shelves
- Info terminals, similar to those using barcodes
- Advertisement screens showing videos to advertise products

[17] All webpages cited in this chapter were accessed on 6th of April 2006.
[18] See http://www.future-store.org/servlet/PB/-s/68lq0912kjivf4hqf0149asnp3spni0/menu/1007054/index.html
[19] See http://www.future-store.org/servlet/PB/-s/68lq0912kjivf4hqf0149asnp3spni0/menu/1007338_l1_yno/index.html

- Intelligent shopping trolleys (integrating the so-called personal shopping assistants; this assistant works together with the customer loyalty card and allows to check the bonus account, displays information about products and advertisements received via WLAN)
- Automated teller systems

In addition to the improvements of the logistic chain and better services within the shop also customer loyalty cards with hidden RFID tags* were issued to the customers until April 2004.[20] In combination with hidden readers* in the store they were used to do personalised profiling on the customers, using the loyalty card. In addition, adjustment of offers to the wishes and needs of the customers is a defined purpose for which this card is used.[21] While this additional purpose was part of the declaration of consent within the contract of the customer loyalty card, the users were not informed about the use of RFID tags* in the cards and corresponding readers* issued at the "Future Store".

Other interesting aspects of this pilot project are technical abilities of the shopping assistant, a tablet PC integrated into the shopping trolley manufactured by Wincor Nixdorf International. They enable multi-channel retail, including the following functions: "The shopping assistant tracks the shoppers' movement using wireless LAN software from Saratoga, Calif.-based Ekahau and displays location-specific personalized shopping lists, favorites and special offers. The system can offer discounts on items related to those put in the cart. It can also trigger in-store signs. So if the shopper puts Pringles in the cart, an ad for Coca-Cola might be displayed. Shoppers who scan all their items can have the information communicated to a cash register wirelessly and checkout quickly."[22]

While it is documented that hidden RFID tags* in the customer loyalty cards were used to activate advertisement displays showing video clips[25], it is not clear whether this was used in the way described above. After the RFIDs in the customer loyalty cards were uncovered by the consumer protection organisations CASPIAN[23] and FoeBuD,[24], the Metro group withdrew these cards and issued traditional ones.[25] Given the ability of the shopping assistant to read traditional customer loyalty cards (via magnetic stripes or barcodes), profiling of customers is still done and adopting advertisements on displays is technically and legally possible.

3.3 Case-study: Usage of RFID Technology in Educational Settings

Denis Royer (JWG)

Besides the many applications of RFID technology in logistics and other related fields, end-user scenarios for educational settings (e.g. museums and exhibitions) are also possible usage scenarios. By adding RFID tags* and RFID readers* to the exhibits, new possibilities with

[20] See http://www.spychips.com/metro/overview.html
[21] See http://www.spychips.com/metro/scandal-payback.html
[22] http://www.rfidjournal.com/article/articleview/489/1/1/
[23] See http://www.nocards.org/
[24] See http://www.foebud.org
[25] See http://www.foebud.org/rfid/metro/

regard to interactive presentation and augmented experience for the visitors arise. Until today, over a hundred museums worldwide are experimenting with ubiquitous technologies (RFID, WiFI, etc) in their exhibitions (Hsi, Fait, 2005).

From the technological perspective, a RFID enhanced educational environment is presented in Figure 4: At the start of his / her museum visit, the visitor gets a RFID token (e.g. as a card or embedded into a personal information device). Furthermore, he or she enrols herself/himself, by storing a user profile into the museums RFID infrastructure. This profile can contain personal information, such as personal interests or the user's age (Fleck et al., 2002; Hsi, Fait , 2005). When passing an exhibit, the user can use the RFID tag* to acquire personalised information about the individual exhibit or trigger the interactive part of an exhibit, when getting into its proximity.

Depending on the individual context of the visitor and the stored profile, personalised information is delivered onto an information kiosk, being attached directly to the exhibit, or onto the user's personal information device. Additionally, the system can track the visitor by taking photos and delivering additional resources. After the museum visit, these can be accessed on a personalised webpage on the Internet (Hsi, Fait, 2005).

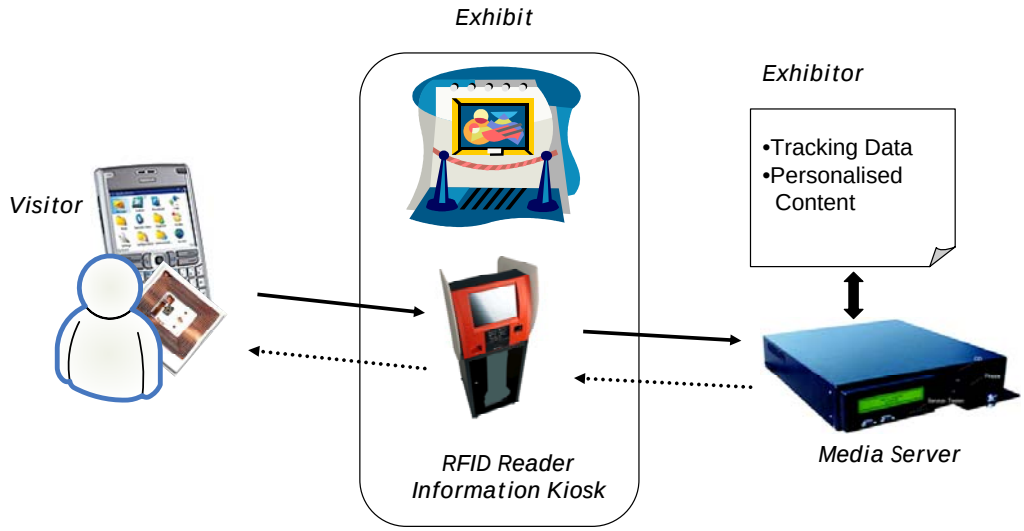

Figure 4: Possible usage scenario for RFID technology in educational settings.

Furthermore, the exhibitors get the opportunity to track the behaviour of their visitors, in order to enhance the exhibition or in order to gather information about the success of the installed exhibits. However, on the one hand this approach is very promising for both parties (visitor, exhibitor), delivering information that could not be gathered by a static exhibition – On the other hand, the requirements towards usability and privacy protection need to be addressed. Especially with regard to the perceived risk of RFID technology, users might not want to use this kind of technology to be tracked when visiting a museum (Hsi, Fait, 2005).

3.4 RFID at the CVS Corporation

Martin Meints (ICPP)

The CVS Corporation, listed at the New York Stock Exchange (NYSE), is the – based on store count – largest pharmacy chain in the United States with 4087 stores. Since May 2002 CVS joined the Auto-ID Center at Massachusetts Institute of Technology (MIT) and began in 2003 with the so-called project "Jump Start" (Garfinkel, Rosenberg, 2005: 201ff.). Target of this project is a full-scale trial of RFID on 10 selected drugs.

There are a number of reasons that CVS involved in RFID. Main reasons are:

- Pharmaceuticals are different from other consumer products such as, e.g., razor blades:
  - They are high value goods.
  - They sometimes have a very long shelf time (up to three or four years before they are sold).
  - In the United States tamper-proofness of pharmaceuticals in the logistic chain and the shops is an issue since the Tylenol scandal in 1982, where Tylenol was adulterated with cyanide and as a consequence a number of consumers died.
- Up to 2002 the EPC* global[26] has not addressed the specific needs of the pharmaceutical industry including
  - Integrating the so far separate National Drug Codes (barcodes) into the EPC*;
  - The need for privacy in the health care sector and
  - The regulatory requirements defined by the U.S. Food and Drug Administration (FDA).

CVS is testing RFID on a per item basis. Drug bottles are RFID tagged* and transported using standard boxes which are also tagged. There are a number of potential improvements in processes that are tested at CVS. The most important are:

- Improvement of drug management at the manufacturer and in the distribution centres of CVS; errors in the delivery such as wrong types or numbers of drugs can be detected easily;
- Improvement in drug management in the stores; the central systems know how many goods are left in the smart shelves even in cases where they are at the wrong place in the shelf (supply management);
- Improved handling of outdates, recalls, returns and damages;
- EPC* stored on RFID can be used to detect certain types of mistakes or manipulations of drugs for example in cases where already used or cloned RFID tags* are used.

[26] EPC global Inc. is a none-profit organisation doing standardisation work with respect to the use of RFID in retail and the Electronic Product Code (EPC*); see http://www.epcglobalinc.org/.

The project comes along with a number of technical innovations. A number of improvements with respect to reader* technology, such as multiple antennas for one reader*or the swivelling of boxes when they pass the reader*, were applied. But accuracy of the reading process still is a problem. Further testing for example of two-way tags that act as a proxy for tags transmitting EPCs* is needed.

CVS does not hand out drugs tagged with RFID to consumers for privacy reasons. Tags are removed in the shop. To ease this, special tags with a perforation to remove the tag from the adhesive pad are used.

3.5 Scenario for social inclusion

Sabine Delaitre (IPTS)

In the framework of the European accessibility policy, the city of Milan (Italy) did some public investments in a navigation support system based on RFID technology so as to equip some administrative buildings of the city. This system will allow disabled people or people with impairment to become self-sufficient and to access to the different offices.

During the first usage period, some problems occurred without damages. However, one day, because of tag-collisions[27], some people got lost and one person has suffered substantial damages. He broke his leg by missing some steps of a staircase. According to the device he though he was on the second floor, but in reality he was on the third one and regrettably, on the second floor there is a staircase with lesser steps then on the third floor. After this incident, it was decided to replace all reader* devices by a new type of reader*, comparable to the "agile reader"[28] in order to solve the collisions problem.

In order to forget this regrettable incident and stimulate the future users, the news paper "Periodico di Milano" wishes to publish an article on the new system by interviewing people.

Two friends, one blind and other one with a low vision are very happy with the new navigation support system. They are able without human assistance to reach any room, any place inside the buildings and relate us their impression:

> *"Before, it was very difficult to progress in a building without a good knowledge of it because most of the signalisation is graphical (even for the toilets). And even if the lifts have in general a Braille conversion of the information related to the floors only very few are equipped with a voice-based interface to indicate you where you are, in the fourth floor or another one selected by other person.*

[27] Tag-collision: Tag collision occurs when more than one transponder* reflects back a signal at the same time, confusing the reader. Source: www.rfidjournal.com

[28] Agile reader: An agile reader is one that can read tags operating at different frequencies or using different methods of communication between the tags and readers. Source: www.rfidjournal.com

Now thanks to the navigation system, we are independent and we can move in complete freedom and safety. It is easy: at the entrance of the building a small device is offered and helps us to progress in the building. This device communicates with all RFID sensors and indicates you by voice interface the right path to follow."*

3.6 Security risks for RFID-enabled profiling

Sabine Delaitre (IPTS)

Marie thinks about her friend Claire who is always fast in adopting new electronic gadgets such as a smart blouse. Marie likes it. It seems really practical. Marie asks Claire whether she may borrow it.

Some days after that, Claire is working at home when burglars break into her apartment. The burglars are surprised to find Claire at home. In the ensuing confrontation, Claire is punched in the face. The burglars get away with only her Personal Wrist Communicator (PWC), her wallet and some jewels that were lying on the table, but the experience of getting robbed will haunt Claire for a much longer time. Moreover, she will now have to train her new PWC from scratch because she did not want to store her profile(s) online, and because the burglars destroyed her home computer which Claire used to back up her PWC.

The burglary and mugging occurred because of an unlucky coincidence of circumstances, i.e. that Marie was wearing Claire's blouse when she went to the park where the criminals happened to be operating. As she was passing by, the gang "read" the RFID tag* embedded in the blouse. As a result, the gang found out (following the brand of the blouse and the publicly available product codes) that the blouse had been sold at a certain shop. The gang hacked the client database of that specific shop to discover Claire's profile (a well-off woman living alone in the richer part of the city) (Knospe, Pohl, 2004). On the assumption that Claire was wearing the blouse, the criminals decided to break into the apartment and to steal whatever luxury goods they could find.

The whole story was uncovered two weeks later when a technician was checking the systems of the shop and found suspicious entries in the systems' log files. He uncovered the hacking and was able to follow up the way the gang broke into the system. He informed the police and made and official report. Investigations are still in progress. Who will carry Marie's costs in the end is a matter of debate between her and the shop's insurance company.

3.7 Scenario for individual/group profiling: the link between privacy and CRM

Sabine Delaitre (IPTS)

Because all garments are equipped with RFID in order to fight against fraud, some shops take advantage of this equipment to perform some follow-up on what it is bought with a view to carrying out CRM (customer relationship management) activities. A first strategy was to make some "flash promotions", i.e. some offers at the right time to the right person (here a

person is group-profiled as belonging to a target group). Group profiling technologies build on similarity (they are a species of categorisation), they are employed to attribute a certain lifestyle to customers and to identify customer preferences.

Flash promotions are a very successful offer type. The sales are significantly increasing.

'Business is business' and some shops decide to do more for boosting the sales to the maximum. They draw up a second strategy which consists in identifying each customer and what he/she is wearing, thanks to the RFID equipment. This new strategy will be based on the use of individual profiling technologies. Thus, in these shops when you enter, the shop is able to recognize for instance the jacket and the pants you are wearing and to suggest you to replace your jacket because you bought it two years ago (in the same shop).

4 Legal Aspects

4.1 Data Protection legislation[29]

Eleni Kosta, Michaël Vanfleteren (ICRI, KUL)

4.1.1 Introduction

In the general frame of Ambient Intelligence, RFID tags* present interest from a data protection point of view. RFID tags* can be used in AmI not only as the medium for the collection of personal data, but also as transmitters of the personal data they contain or as tracking devices for the location of natural persons. All the aforementioned functions of RFID tags* can be used for profiling purposes.

The answer to the question, whether we should use the term 'data protection' or 'protection of privacy' was given by the European Data Protection Supervisor (hereinafter EDPS), when commenting on the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data (Convention No. 108). According to the EDPS "[t]he Convention deals with 'data protection' as protection of fundamental rights and freedoms of individuals, in particular their right to privacy, with regard to the processing of personal data relating to them". This demonstrates that 'data protection' is wider than 'protection of privacy', since it also relates to other fundamental rights and freedoms of individuals, and at the same time more specific, since it only deals with the processing of personal data. In this context one should realise that many activities in the public or the private sector nowadays generate personal data or use such data as input. The real objective is, for that reason, to protect individual citizens against unjustified collection, storage, use and dissemination of their personal details."(European Data Protection Supervisor, 2004: 12) Based on this argumentation we decided to focus on the protection of personal data during their collection and processing in AmI.

Although they have sometimes been labelled as the next-generation of bar codes, RFID systems* offer much more in that they can track items in real-time to yield important information about their location and status (ITU, 2005). From the definition of 'personal data'[30] it becomes clear that only information relating to an identified or identifiable natural person (data subject) qualifies as personal data and such data will be the main focus of our analysis in AmI environments. Recital 26 of the Data Protection Directive stipulates that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". As the Working Party 29 has already pointed out it is essential in the case of data collection through RFID tags* first of all "to

[29] We refer to deliverable 7.3 which contains an extensive analysis of the European legal framework regarding profiling, with special attention to the data protection regime.

[30] Art. 2 (a) 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, hereinafter the "Data Protection Directive", Official Journal, L 281/31 – L 281/39.

determine the extent to which the data processed relates to an individual and [secondly] whether such data concern an individual who is identifiable or identified."(Art. 29 Data Protection Working Party , 2005: 8).

Therefore, as already noticed in section 2.3, RFID tags* can also be used to identify persons directly or indirectly. More specifically, as a rule of thumb it can be said that the RFID tags* used in an AmI environment contain in most cases personal data. For instance the RFID tags* that are used for the storage of personal information, such as in identification documents, always contain personal data. The same shall apply for RFID tags* that although they don't contain personal data can easily be linked to a natural person, like RFID tags* included in loyalty cards. In this case the linkage can be completed by simply linking the reference information on the loyalty card with the information in data bases, such as the credit card data of the data subject (Legal IST, 2006, 19ff). A practical example can be found in the Metro case-study presented earlier where the shopping company issued loyalty cards with embedded hidden RFID tags* which allowed personalised profiling on the customers (cp. section 3.2). However, more unclear is the case when an RFID tag* cannot immediately be linked to an individual.

Several issues arise regarding cases when RFID tags* cannot be immediately linked to individuals. The key question will be what are the "means likely reasonably to be used"[31] in order to identify a natural person? How far can we go in our effort to link the data stored on the RFID tag* to a natural person and therefore apply the data protection legislation on them? An additional issue is that the Member States have a different interpretation of the term 'personal data'. How can we ensure that a uniform pan-European approach will be adopted?

4.1.2 Collection and processing of data

In an AmI environment vast amounts of personal data are collected from RFID tags* and are further processed for various purposes. Therefore it is essential to differentiate between legitimate and non legitimate collection and processing of such data. While during legitimate collection and/or processing of personal data the legal requirements set out in the European legal framework on data protection need to be respected, in the case of unauthorised collection and/or processing of such data, additional countermeasures need to be deployed.

4.1.2.1 Collection and/or processing of personal data

Personal data can be collected legitimately through RFID tags*, as long as the collection takes place for "specified, explicit and legitimate purposes"[32] and as long as the personal data is "processed fairly and lawfully".[33] Further processing of the data is allowed only in a way which is compatible with those purposes.[34] When personal data are collected via an RFID

[31] Recital 26 Data Protection Directive
[32] Art. 6 (b) Data Protection Directive
[33] Art. 6 (a) Data Protection Directive
[34] Art. 6 (b) Data Protection Directive

enabled loyalty card, such purposes can be the provision of better services, discount prices or personalised offers. In case the processing of personal data that are collected by the RFID tags* is "necessary for the performance of a contract to which the data subject is party",[35] the consent of the data subject is not needed.

The most common basis for the collection of data, however, remains the provision of the unambiguous consent of the data subject[36]. The consent of the data subject needs to be a freely given, specific and informed indication of the wishes of the data subject, by which he signifies his agreement to a personal data relating to him being processed[37]. In order to have a 'freely given' consent of the data subject, it is important to examine how much choice is in fact given to him. Article 29 Working Party (2001; 2002), has for instance considered that the consent given by an employee to the use of his personal data "as a part of an employment contract is not a 'freely given' consent" (Jay, Hamilton, 2003: chapter 3 – 39). When it comes to RFID, the data subject should be given the possibility to really *choose* that he wants to use RFID tags*. In simple words the data subject should have the alternative to choose another way of enjoying the offered service, even if that alternative does not have all the advantages and benefits that come with the RFID tags*. For instance the customers should be given the possibility to chose between tagged and non-tagged products, even if the latter will not offer them the possibility to receive information about discounts on other items related to those put in their cart (Metro Future Store case). Secondly, it should be specific, meaning that the data subject needs to be clearly informed what he is consenting to. Finally the consent of the data subject shall be informed. The data subject shall consent to the collection and processing of his personal data after he is informed by the controller or his representative on the identity of the controller (and of his representative), the purposes of the processing for which the data are intended, as well as about the recipients of the data, about the fact whether replies to questions are obligatory or voluntary and finally about his right to access the data, to ask for their rectification, erasure or blocking[38] and the right to object to the collection of his data.[39] Breach of this legal requirement can be found in the case of the Metro Future Store in Rheinberg. In the declaration of consent within the contract of the customer loyalty card it is mentioned that "adjustment of offers to the wishes and needs of the customers is one of the purposes for which this card is used".[40] However this clause is not written in a clear way so that it cannot be understood by all the customers and the consent of the customers is not given lawfully.

When personal data are collected via RFID tags* in an AmI environment, the data subject has the right to be informed in a clear and intelligible way about the form of the data undergoing processing as well as about the means and precautions the data controller has taken to adhere to the data protection principles. Furthermore, in cases of automatic processing of the data, the data subject is entitled to know the logic involved in this.[41] In the example of the Metro

[35] Art. 7 (b) Data Protection Directive
[36] Art. 7 (a) Data Protection Directive
[37] Art. 2 (h) Data Protection Directive
[38] Art. 10 Data Protection Directive
[39] Art. 14 Data Protection Directive
[40] 3.2 Case Study: The Metro future Store in Rheinberg
[41] Art. 12 Data Protection Directive

Future Store for instance the RFID tags* in the customer loyalty cards were used to activate advertisement displays. However, the procedure and the logic followed for this was not known. It goes without saying that the procedure of collecting data shall be transparent for the additional reason that in this way the criteria used for choosing the specific data as appropriate can be easily checked.

In the context of profiling special consideration needs to be given to Art. 15 (1) of the Data Protection Directive. This article gives the right to every individual "not to be subject to a decision which produces legal effects 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.". Therefore, when profiles are created based on data that are collected via RFID tags*, completely automated processes shall be avoided. However, this prohibition seems at odds with the logic of adaptive autonomic profiling, as discussed in section 2.1, since most decisions will be taken by machines in a process of machine to machine communication. To find out to what extent such M2M decision-making processes contain decisions that effectively 'produce legal effects concerning a data subject or significantly affect him', would require a measure of transparency that is not yet available. Adapting an environment presumes a contractual relationship between a service provider and a consumer, which thus has legal effect. Depending on the type of 'social sorting' that is produced by autonomic profiling these processes may have a profound impact on the distribution of risks and opportunities, thus significantly affecting a person.

4.1.2.2 Services based on location data

In an AmI environment, RFID tags* are used mainly as a means for the tracking and tracing of people. When services based on the location of the data subject are offered we need to check whether Article 9 of the e-Privacy directive applies. The sector-specific provisions of the ePrivacy Directive and therefore Article 9 as well apply to publicly available electronic communications services or when the service is offered over a public communications network. It is obvious that the prerequisites of a communication[42] as set down in the definition of the term in Article 2(d) of the e-Privacy directive need to be fulfilled. Otherwise only the more general provisions of the data protection Directive apply.

However, the regular function of RFID tags* neither presupposes a publicly available network nor demands a provider for the provision of the service (Legal IST, 2006: 20). If this is the case, article 9 of the e-Privacy directive does not apply. However, when the RFID tag* enables the provision of a value added service, then the aforementioned article is applicable. In such a case, when location data relating to users or subscribers are processed, they "may only be processed when they are made anonymous, or with the consent of the users or

[42] Communication means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information (Art.2 (d) ePrivacy Directive).

subscribers to the extent and for the duration necessary for the provision of a value added service".[43] Furthermore, "[t]he service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time".[44]

In the Metro Future Store 'the shopping assistant tracks the shoppers' movement using wireless LAN software and displays location-specific personalized shopping lists, favourites and special offers. The system can offer discounts on items related to those put in the cart. It can also trigger in-store signs.[45] When the customers give their consent to use their loyalty card (given that they are aware of the RFID tags* and readers*) in connection with the shopping assistant, they accept the legitimate processing of their data in order to receive the personalised information. Similar is the case in the Museum scenario, as the user creates his/her own personal profile into the museum's RFID infrastructure in order to receive more personalised information. In both aforementioned cases the RFID tags* enable the provision of value added services and therefore Article 9 ePrivacy directive shall apply**.**

4.1.2.3 Obligations of the data controller

The data controller is the one that "determines the purposes and means of the processing of personal data".[46] For that reason in each specific case we need to apply this definition in order to determine who is the controller. As a rule of thumb it can be said that the data controller is the 'tag deployer' (Legal IST, 2006: 21), the one that decides the purposes for which the RFID tag* is used, which data shall be collected and whether these data will be further processed. In the scenario of the Museum for instance, the responsible department of the museum that decides on the personal data of the visitors (for which purposes they are collected and processed, how this can be achieved etc.) is the data controller and bears the burden of complying with the data protection legislation.

In an AmI eEnvironment it is very important to identify the controller of the data in order to specify the natural or legal person that needs to ensure the respect of the principles related to lawful processing of data. The personal data shall be collected[47] and processed fairly and lawfully. Therefore the collection of data by illegal means violates the fairness principle. Such violation occurs in the Metro Future Store scenario where hidden RFID readers* and hidden RFID tags* on the loyalty cards are used, as well as the unauthorised reading of the RFID tag* of Claire's blouse by the burglars (Punie et al., 2006). In the former case of the Metro Future Store, specific pictograms or signs should be placed in the store indicating the

[43] Art. 9 ePrivacy directive.
[44] *Idem*
[45] http://www.rfidjournal.com/article/articleview/489/1/1/
[46] Art. 2 (d) Data Protection Directive
[47] One should be reminded at this point that the collection of data is included in the general term 'processing of data'.

presence of both RFID tagged products and RFID readers* in the supermarket departments or shelves (Van Eecke, Skouma, 2005: 175).

According to Art. 6 (c) of the Data Protection Directive, the collected data shall be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". In the example of loyalty cards, identification data and contact details are needed for the offering of the commercial benefits to the customers. However, it is quite common in practice that further information regarding the customers as well as their family members is asked, such as their education, profession, preferences etc. (Italian DPA, 2005). Notwithstanding that this practice is broadly used, it comes in opposition to the data minimisation principle as well as the proportionality principle that requires the data controller to collect and processes as few personal data as possible. Furthermore, the data shall be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[48]

Furthermore, the data shall be "accurate and, where necessary, kept up to date".[49] The processing of wrong information will lead to inadequate profiling and will end up in profiling mismatches. In a 'worst-case scenario' processing of inaccurate information can lead to harming a data subject, based on wrong information, such as in the case of Clair.

As already mentioned above, the data controller needs to respect the finality principle, which means that the data shall be collected and processed for specified, explicit and legitimate purposes and further processing of the data is only allowed for purposes compatible with the initial ones.

The data controller shall ensure that the rights of the data subject are respected. In the frame of AmI when the data subject exercises the right to know which of his data are processed, as well as the right to access these data, the controller has a difficult task to carry out. The data are stored in several places (tag, central database etc.) and the data controller must provide information about *all* the places where data are stored. In this way the data subject will be able to fully exercise his right of rectification or deletion of data, when necessary.

4.1.2.4 Future of RFID in AmI

The application of the concept of personal data to emerging technologies raises new legal issues, since the meaning of two important elements of the definition of personal data is no longer self-evident. These two elements are 'relating to' and 'identifiable'. The application of these elements is challenged by new forms of processing like web services and by an erosion of the traditional technological barriers (power limitations, limited transmission range, isolated data, etc.). As seen in this report, this is well-illustrated by the growing use of RFID

[48] Art. 6 (e) Data Protection Directive
[49] Art. 6 (d) Data Protection Directive

tags* and the massive development of communication networks which, as underlined by the EDPS have the following impact:

- All tagged objects become a collector of personal data;
- The 'presence' of these smart objects as well as individuals who carry them is characterised by its 'always on' nature; and
- The resulting cascade of data continuously feeds an enormous amount of stored data (European Data Protection Supervisor, 2005).

The core concept in the European data protection legislation is 'personal data'. However, as indicated in section 2.1 the protection needed as a consequence of profiling technologies in an AmI environment regards the application of *group* profiles that may have been constructed without the use of personal data (either because the data have been anonymised or because the profile has been constructed without the use of data of the person it is applied to, see FIDIS deliverable 7.2 section 3 on the construction of group profiles). For this reason, next to Identity Management Tools that allow the data subject some kind of control over the leaking of his personal data, the application of group profiles requires new tools to access the knowledge (profiles) constructed by the profiling by data controllers.

4.2 Liability Issues

Colette Cuijpers (TILT)

4.2.1 Introduction

In the previous paragraph an illustration is given of possible privacy infringements within AmI-systems. These infringements can lead to damages for which the injured party might desire compensation. In the SWAMI (De Hert et al., 2006) research, problems regarding compensation for damages caused by privacy infringements in an AmI environment have already been addressed. This article incorporates the findings of the SWAMI research. However, the scope of liability issues within AmI environments will be extended beyond privacy. From the scenarios sketched in the third chapter it becomes clear that a (technical) malfunction within an AmI environment, as well as the use of AmI-systems or even the mere 'living within' such an environment can lead to a variety of damages.

As mentioned in chapter 2, RFID systems* can be understood as forerunner technologies or basic enablers for AmI. As RFID systems* already raise enough liability questions, those related to the more complex AmI-system are not elaborated upon. In this respect, the liability regime regarding service providers as regulated by the E-commerce directive is left out of the discussion as the role of these providers is more related to AmI-systems then with RFID systems*.

Regarding privacy in relation to RFID systems*, damages can for example result from the accumulation of data in central servers, the (concealed) processing of personal data on a RFID tag*, the possibility that tags are read by third parties without the tag holder[50] being aware of this, and the tracking and tracing of tagged persons. In this respect the SWAMI research states that it is desirable to further examine the need for specific rules on the liability for infringement of privacy and data protection law, including security infringements. This statement being true, nevertheless it leaves you wondering whether the need for general unified liability rules might not be even more desirable? This question will be central to this contribution. In order to answer this question, the current liability regime and its main problems regarding the application of this regime within RFID systems* will be described.

4.2.2 RFID systems*

From the description in the second chapter of a RFID system*, it already becomes clear that it involves a lot of different components. In this respect mention is made of tags, corresponding readers*, computing device(s), an infrastructure for data transport from the reader* to the computing device, software, reference database, interfaces to external data and services, and components to use the results of the matching process.

Within the RFID system*, different parties can be responsible for the different components. Even with regard to each and every component there might be different parties involved in the production and functioning of these components. This leads to a very complex structure of products and parties and to opacity with regard to legal responsibilities if damages occur due to a malfunction, or even the mere (mis)use of the RFID system* (cp. the scenarios of sections 3.5, 3.6 and 3.7). In an AmI environment there might even be more complicating factors such as the use of intelligent agents. As already explained, this contribution will be limited to liability problems regarding RFID systems*.

In part, the question as to who is liable for inflicted damages is not influenced by (the use of) RFID systems*. For example, the case of the Metro Futures Store. In this case, the store is liable for the infringement of privacy caused by the customer card. Not so much the use of the RFID tag*, but the concealment of the use of the tag as well as the use of the gathered data led to the infringement of the privacy. Any means of gathering, storing and analysing personal data in a concealed manner, would have made the store liable for the privacy infringement. However, RFID systems* do raise a lot of liability issues that are difficult to solve, because of the complexity of these systems. In this respect the following remark in the SWAMI research is illustrative:

> *"Nearly in every situation regarding consumer relationships, the factual situation might be very complex (e.g. in case of data mismatch and access refusal, the client is faced with a problem caused by a complex technological system, which has been*

[50] I deliberately do not speak of tag owner, as this is a legitimate legal issue to explore in itself. In buying a tagged product, do I become the owner of the tag? So with tag holder I mean the person, directly or indirectly, linked to the tag.

> *constructed by the joint efforts of several actors). It can be very troublesome for a user to point at the party who is actually responsible for the damages caused, especially if (s)he does not know which parties were actually involved in the service/software creation and delivery."* (Friedewald et al., 2006: 151)

As an example, reference can also be made to the scenario for social inclusion in which the issue of tag-collision is addressed.

So, the different components as well as the variety of involved parties lead to a complex context for assessing liability. The opacity and lack of predictability with regard to the (mal)functioning of the system makes it even more intricate. Technical specifications will be a decisive factor with regard to questions like:

- How big are the chances of tag-collision?
- How big are the chances of miscommunications between tags and readers*?
- How much influence do different tags and different readers* bear on each other?
- What can be the consequences of this influence?
- Can security with regard to internal and external reference data within the RFID system* be guaranteed?[51]

Even though these questions will be different for each and every RFID system*, they do in general justify legal research into the question as to whether current liability regimes are a sufficient means with regard to RFID systems* to allocate legal responsibilities and to be used as a tool to compensate for inflicted damages caused by (the use of) the RFID system*.

4.2.3 Different liability regimes; no unified law on liability

In the European Union there is no unified general law on contractual, nor on non-contractual liability. If a RFID system* completely consists of components from one country, and all parties involved reside in that same country, the lack of unified rules regarding contractual and non contractual liability might not be that much of a problem. As it is more likely that a RFID system*, and even more so an AmI-system, consists of components and involves parties from all over the world, the lack of a unified legal framework might be a highly complicating factor.

Without a European legal framework, liability for damage caused by RFID systems* is to a large extent regulated by national law. Within the European Union several projects are, or have been, running with regard to the harmonization of tort law, the harmonization of the law on contract and even on a 'European Civil Code'. From this research it becomes clear that, within the European Union, a legal "rift" exists in liability law. Not only between Common law-countries (e.g. UK) and Civil law-countries (e.g. France, Germany) a lot of differences in

[51] In this respect a link can be made with paragraph 2.4 concerning the security of RFID systems.

the laws on contractual and non-contractual liability exist.[52] Also the different civil law regimes regarding contractual and non-contractual liability display a large variety of legal rules. In the research projects regarding European Private Law, the question as to whether this "rift" should be solved by European legislative measures is answered in an affirmative manner.[53] However, until now, none of these research projects has lead to legally binding regulations.[54]

The absence of unified liability rules leads to complex questions as to applicable law and competent forums. At the European level, Private International Law issues are regulated by the Rome Convention on the law applicable to contractual obligations[55] and the Brussels Regulation on jurisdiction and enforcement of judgements.[56] Even with the existence of this legal framework a lot of practical problems remain, which will not be elaborated upon in this contribution.[57] The issue is just addressed to illustrate the desirability of unified liability rules, as within a RFID system* it is already complicated enough to trace a malfunction and the responsible party, without having to assess what liability rules apply and what forum to address. Also the SWAMI research states that:

> *"Clear rules determining the law applicable between the parties are an important guarantee of the legal certainty. They allow to predict what rules (i.e. which law) will apply to his activity beforehand, and thus to know which rules to obey. Private international law is an important element which can facilitate the adherence to the legal requirements. Clear rules on the applicable law and the choice of jurisdiction to determine the case can facilitate the court actions and create the impulse to enforce the law by individuals who suffered damages."* (Friedewald et al., 2006: 162 – 163)

[52] For this remark regarding tort law see: European Group on Tort Law, www.egtl.org. For Contract Law see (Von Bar et al., 2002: 183 – 248).

[53] In particular there are two groups doing research in this area. Firstly, the European Group on Tort Law, which has published a book called: "Principles of European Tort Law, Text and Commentary. Springer Wien NewYork, 2005. http://www.egtl.org/. Secondly, the European Research Group on Existing EC Private Law (Acquis Group) http://www.acquis-group.org/

[54] The Principles of European Contract Law (PECL), even without a legally binding nature, do have some legal relevance. A choice of law for the Principles can be made in case of an international contractual relationship to overcome differences in national legislation. The choice for the PECL can be to avoid difficulties in agreeing on a national system of law. If no explicit choice of law is made in a contractual international relationship the courts might as well apply the PECL. The justification for applying the Principles is that it is hoped that the Principles will furnish a more appropriate basis than any system of national contract law for the adjudication of an international contract (Busch, D., 1998).

[55] Convention of Rome on the Law applicable to contractual obligations opened for signature in Rome on 19 June 1980 (80/934/EEC), OJ L 266, 09/10/1980 p. 0001 - 0019.

[56] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 012, 16/01/2001, p. 0001 – 0023.

[57] For an insight into these problems reference can be made to the already mentioned research projects into unifying legislation on contractual and non-contractual liability and on the development of a European Civil Code, for example www.egtl.org, www.acquis-group.org and www.sgecc.net. Also the SWAMI research gives some more insight in the complex legal framework regarding Private International Law, see chapter 3.

Even though there is no general harmonisation of liability law within the European Union, there are several European directives regarding liability in specific areas or concerning specific parties. Regarding RFID systems*, relevant liability clauses can for example be found in the E-commerce directive, the directives concerning product liability, and the unfair contract terms directive.[58] Even though these regulations bring some clarity to specific legal relationships, they do not constitute a harmonized legal framework regarding liability. Also the level of harmonization established by the mentioned directives is not unambiguous as differences in interpretation, as well as differences in national implementation law, remain. In the following paragraph, a short description is given of the most important directive with regard to RFID systems*, the directive on defective products. The description of this directive will illustrate the above mentioned problems.

4.2.4 Different liability regimes; Directive on defective products

4.2.4.1 Products, software and services

Liability for defective products is regulated by Directive 85/374/EEC as amended by Directive 1999/34/EC.[59] Besides the lack of a unified legal framework regarding contractual and non-contractual liability within the EU, the scope of the directive on defective products is one of the reasons for differing liability regimens regarding RFID systems*. As described in the first chapter, a RFID system* consists of products as well as software and is able to provide services. However, from a European legislative perspective, these three issues are not dealt with by the same liability regime as services fall outside the scope of the directive for defective products[60] and with regard to software it is doubtful whether this falls within the definition of a 'product'. From the contents of the directive it becomes clear that not only the differing liability regimes might lead to problems when harmed persons try to get compensation for inflicted damages caused by a RFID system*. The following paragraphs will address the most eminent problems in this respect.

4.2.4.2 The definition of a product

One of the problems regarding liability for defective products and RFID systems* is the uncertainty with regard to the definition of a 'product'. Article 2 of the Directive states: "*For*

[58] Council Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17/07/2000, p. 0001 – 0015. Council Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 14, 04/06/1999, p. 0020 – 0021. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 07/08/1985, p. 0029 – 0033. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 095, 21/04/1993, p. 0029 – 0034.

[59] Directive 1999/34/EC amended Directive 85/374/EEC by redefining "product' as all movables even if incorporated into another movable or into an immovable. In the original Directive, primary agricultural products and game were excluded. However, Directive 1999/34/EC extended the scope of Directive 85/374/EEC so that it now includes primary agricultural products (such as meat, cereals, fruit and vegetables) and game (Delaney, Van de Zande, 2001: 2).

[60] Until now all efforts to establish a directive on defective services have failed.

the purpose of this Directive, 'product' means all movables even if incorporated into another movable or into an immovable. 'Product' includes electricity." This definition does provide room for interpretation leaving uncertain whether software must be qualified as a product. Due to this uncertainty differences in interpretation can emerge between the Member States of the European Union. The problems this can impose with regard to solving liability conflicts arising out of (trans-border) RFID systems* are obvious. For now, it seems that the view taken within the European Union is that software is not covered by the definition of 'product'. However, as is highlighted in the SWAMI research, from a technological perspective it is difficult to distinguish between hardware and software. The SWAMI research also refers to the growing number of products with embedded software, which do fall under the regime of the directive.[61] This makes the distinction between software and products even more doubtful. Therefore the question is raised why such a distinction should be drawn from a legal perspective?[62] The SWAMI research goes as far as to propose to consider an *explicit provision providing for the strict liability for software.* The researchers are aware of the resistance against such a provision founded on the argument that such a provision would threaten industry and innovation:

> *"Since, in the opinion of the computer specialists, the software is never defect-free, the strict liability would expose software producers unfairly to the damages claims. Thus, the degree of required safety of the programs is the policy decision. Strict Liability could also impede innovation, especially the innovation of new, experimental and life-savings applications. Others argue that strict liability might increase the software quality by making producers more diligent, especially, in properly testing the product."* (Friedewald et al., 2006: 152)[63]

In the SWAMI research mention is also made of the difficulty to draw the line between software and services. As several efforts to establish a directive for defective services did not make it, strict liability currently does not apply to services. Service liability is regulated by the national laws.[64] With regard to strict liability for services, the same kind of reservations are used as with regard to strict liability for software; it would impede innovation and creativity and put too much of a burden on the service provider. Whether these reservations are legitimate can be disputed, especially as exemptions, such as the state of the art defence as described in paragraph 4.2.4.4, can offer relief for software producers as well as for service providers.

With regard to Internet service providers some rules regarding liability have been harmonized by the E-commerce directive.[65] Liability of these providers for mere conduit, caching and

---

[61] SWAMI referring to (Reed, Welterveden, 2000: 99).
[62] SWAMI referring to (Hilty, et al., 2005: 269).
[63] SWAMI referring to (Alheit, 2001: 204); Singsangob, (2003: 113) and (Desai et al. 2002).
[64] As the basis for liability the contractual liability or the fault-based tort liability applies (Magnus, Micklitz, 2004, Part D: 62).
[65] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), p. 0001 – 0016.

hosting is regulated in the articles 12 to 14. Also the electronic signatures directive[66] contains in article 6 a specific liability clause with regard to certification-service-providers. These provisions will not be elaborated upon as they are not that influential in relation to RFID systems*.

4.2.4.3 Damage and proof

The Directive on defective products introduces the concept of strict liability (without fault) on the part of the producer in favour of the victim with regard to defective products that cause personal injury or property damage. Even though the directive favours the victim in this respect, an important disadvantage for them remains as the directive places the burden of proof on the injured party insofar as the damage, the defect, and the causal relationship between the two is concerned.[67] As the Directive provides for liability without fault, it is not necessary to prove the negligence or fault of the producer or importer.

For the purposes of Directive 85/374/EEC 'damage' means damage caused by death or by personal injuries; and damage to an item of property intended for private use or consumption other than the defective product, with a lower threshold of ECU 500.

Even though the directive does not apply to other kinds of damages, it does not in any way restrict compensation for non-material damage under national legislation.

The question is which types of damages are caused by RFID systems*? As mentioned before, today RFID systems* are mostly used in SCM, for the identification of objects. In this respect, the probability for substantial damages for the parties involved might not seem that urgent. For example, if you look at the scenario of the Metro Future Store, severe damages are not that likely. Also the scenario regarding usage of RFID technology in educational settings does not necessarily require an analysis of liability risks as they are likely to be minimal. However, if we broaden the scope of supply chain management outside the borders of one specific store, liability risks become clearer. For example in case of dislocation of perishable goods, caused by a malfunction in the RFID system*, it is not that hard to imagine this resulting in a huge amount of damages.

Also with regard to the CVS case concerning RFID labelling of drugs, liability issues might come into play. Even though the scenario mentions a decrease in errors in the delivery because wrong types or numbers of drugs can be detected easily, it can also be imagined that miscommunications within the RFID system*, could lead to life threatening situations. Also the scenarios of social inclusion, as well as the one on security risks for RFID-enabled profiling, provide examples of RFID systems* causing personal injury.

Another example of a completely different kind of damage can be illustrated with the CVS scenario. In this scenario it is described that no drugs tagged with RFID are handed out to consumers for privacy reasons. Acting against this principle can lead to severe cases of social

[66] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19/01/2000, p. 0012 -0020.
[67] Article 4.

exclusion, leading to possible material damage (e.g. exclusion of insurance) but also immaterial damage (e.g. stigmatisation).

Another important issue that must not be forgotten is that current applications of RFID systems* do not preclude the possibility that future applications of these systems can lead to even more severe damages.

As already can be concluded from the discussion with regard to RFID and the invasion of privacy, not only a malfunction of the RFID system* can lead to damage, but also the use of such a systems or even the mere fact that you 'live' within an environment in which you are submitted to RFID systems* without the possibility to withdraw. For instance because you are not aware of the fact that you are carrying a tagged item.[68] It can also be the case that the tag is connected to everyday necessities such as money in your wallet and your identity card, items you cannot leave at home for practical or even legal purposes. An illustration of the far reaching consequences that a RFID system* (or better environment) can have is given with the scenario described in section 3.6 on the security risks of RFID-enabled profiling.

So the foregoing illustrates the vast variety of damages that can occur regarding RFID systems*. However, illustrating possibilities of damage is something completely different from proving the damage. Even though damage can be eminent, it may still be very hard to put a price tag to the damage caused, which can be grounded on material evidence. As already mentioned, proving the fault, and proving the link from the fault to the damage might already be a bridge too far, due to the complexity and opacity of a RFID system*.

In this respect the SWAMI research proposes three possible solutions. First of all the SWAMI research mentions the burden of proof as one of the biggest problems in the liability action. It is stressed that the unawareness of data processing within the complexity of the AmI environment creates an inequality of the information flow which often makes it impossible for users to prove the fault and who is responsible for it, and thus the causal link between the fault and the damage. Therefore the SWAMI research recommends reversing the burden of proof, which solution is also adopted in the field of antidiscrimination and intellectual property laws, as well as in national tort systems (Magnus, Micklitz, 2004). Again this recommendation is aimed at privacy and data protection in particular, while such a reversal can be interesting in a much broader context. With regard to directive 95/46/EC implicitly another solution is proposed by SWAMI. The principle of article 23 Directive 95/46/EC, stating that any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the controller for the damage suffered, could be explained as meaning that any act of unlawful data processing gives the right to damages, even if no (eminent and measurable) damage is inflicted. However, this explanation might be outside the boundaries of what is actually meant by Article 23.

[68] For example the Future Metro scenario in which the customers were not aware of the RFID-tag in their customer loyalty card.

Secondly it is proposed to introduce fixed damages which would provide clarity as to the damages to expect and therefore could possibly have a deterrent effect.

A third solution, mainly given with regard to claims that, due to the limited amount of damage, are not suitable to bring to court, concerns the option to allow consolidation of small claims of individuals, for example group consumer actions.[69]

4.2.4.4 State of the art defence

In article 7 of the Directive on defective products several exemptions are listed to exclude producers from liability. One of these exemptions concerns the so called state-of-the-art defence: The producer is freed from all liability if he proves:

> "*that the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable the defect to be discovered.*"[70]

The SWAMI research indicates that it is argued that such a defence, which is at the discretion of the Member States according to article 15, will always be possible since, due to the complexity of the 'code', software will never be defect free.[71]

4.2.4.5 Joint and several liability[72]

One of the advantages of the Directive on defective products is that it establishes joint and several liabilities of all operators in the production chain[73] in favour of the injured party, so as to provide a financial guarantee for compensation of the damage. Where the producer of the product cannot be identified, each supplier of the product shall be treated as its producer unless he informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product. The same shall apply, in the case of an imported product, if this product does not indicate the identity of the importer referred to in paragraph 2, even if the name of the producer is indicated.

The Directive does not provide for a cause of action. This is left to the Member States. Product liability cases are tried in national courts under national laws (Delaney, Van de Zande, 2001: p. 1). From article 13 of the Directive it becomes clear that the Directive shall not affect any rights which an injured person may have according to the rules of the law of contractual or non-contractual liability or a special liability system existing at the moment when the Directive is notified. The producer's liability is not altered when the damage is caused both by a defect in the product and by the act or omission of a third party. However,

---

[69] For example the Dutch Civil Code, article 3:305a.
[70] Article 7 (e).
[71] SWAMI referring to (Alheit, 2001: 204).
[72] Article 5: Where, as a result of the provisions of this Directive, two or more persons are liable for the same damage, they shall be liable jointly and severally, without prejudice to the provisions of national law concerning the rights of contribution or recourse.
[73] Article 3 of Directive 85/374/EC gives a very broad definition of the 'producer'.

when the injured person is at fault, the producer's liability may be reduced.[74] From article 12 it becomes clear that the provisions of the Directive on defective products are mandatory in nature as producers may not, in relation to the injured person, limit or exempt liability arising from this Directive.

4.2.5 Conclusion

As illustrated by the scenarios in Chapter 3, RFID systems* can cause substantial damage. The current legal framework regarding liability does not seem to provide an adequate system to compensate for inflicted damages caused by (the use of) a RFID system*. Not only the technicalities play an important role, but also the lack of legal uniformity. From a technical perspective interesting questions arise with regard to the predictability of malfunctions and the probability of these occurring. Also the traceability of malfunctions and responsible parties within the system are important factors regarding the allocation of legal accountability. Another important technical issue to address is the possibility to 'turn off the system'. As mentioned before, today's RFID tags* do not stop to respond to readers* when the product was bought by a customer and leaves the supply chain unless special measures to destroy or deactivate the tags are taken. An illustration of far reaching consequences this can have is given by the scenario on the burglary of Clair as described in section 3.6.

In this respect interesting questions from a legal perspective arise. For example the question as to whether there is a right to 'withdraw from the system' and questions relating to consent to 'living' within the system. For example, can mere 'participation' in an AmI environment be viewed as 'permission' by the users of RFID-technology to submit persons to this environment or technology?

The foregoing supports the conclusion that further research into liability and RFID systems* and AmI-environments is needed from different scientific angles.[75] The legal research could start with the fundamental problems described in this contribution that arise from the lack of unified liability rules or from the lack of unambiguous harmonization or interpretation of existing liability rules.

4.3 Implications for Criminal Law

Bert-Jaap Koops (TILT)

The implications of RFID for criminal law are an unexplored field. Clearly, numerous issues in both substantive and procedural criminal law may surface. Due to the relatively small and sector-specific scale on which RFID has been implemented so far, however, these issues have not yet been really encountered in practice. Nor do the cases and scenarios sketched in the previous sections pose clear questions with respect to criminal law, at least on the face of it. Perhaps surprisingly, the criminal aspects of RFID have also been little studied in academic

[74] Article 8.
[75] Besides the technical and legal perspective that are mainly reflected upon in this contribution, interesting questions also arise out of ethical, sociological and economical perspective.

literature or in civil-society reports – the main focus in the academic and societal debate so far has been on privacy issues.

This section sketches the criminal-law implications of RFID in general. It is exploratory and tentative, and should be regarded as a first attempt to list the various criminal issues that may arise when RFID, and ultimately Ambient Intelligence, are implemented on a wide scale. Since criminal law is still to a considerable extent a matter of national legislation, it will not be possible to comprehensively refer to all relevant criminal-law provisions, since these largely depend on the specifics of the laws of the various states. Still, the EU Framework Decision on attacks against information systems[76] (hereafter: Framework Decision) and the Council of Europe's Convention on Cybercrime (hereafter: Cybercrime Convention)[77], give at least some footing.

4.3.1 Substantive criminal law

As all new technological inventions, RFID can be abused by criminals. It can be used as a means to facilitate crime, such as stalking. On the other hand, RFID is also useful for preventing crime, for instance, forgery or theft. In this respect, RFID is simply another tool to identify people or objects and in that respect, it plays a part in preventing or committing crime. Still, it is important to pay attention to the criminal potential of RFID, since criminals might exploit unsuspected vulnerabilities with considerable damage as a result. For instance, researchers of the Free University in Amsterdam have shown that a virus on an RFID tag* can infect a back-end database through the RFID reader*, depending on certain vulnerabilities in the RFID software (Rieback et al., 2006). More research into the risks that RFID systems* present as a tool for attacking computer systems and networks is therefore recommended, and companies implementing RFID should take care to build in adequate protection.

Equally interesting are the crimes committed against RFID, i.e., that have RFID as an object. Of course, stealing an RFID tag* is theft, and destroying a tag is damage to objects, but there are ways in which RFID as the object of crime raises questions.

When someone manipulates an RFID tag* with malicious intent, what crime would this constitute? Here, a major issue is whether an RFID tag* qualifies as a computer or information system. This will depend on the type of RFID tag*: some have processing power and would probably fulfil the definition of a computer system. The definition of the Framework Decision of an information system in art. 1(a) is:

> *'any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.'*

[76] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *Official Journal* L 69/67, 16.3.2005.
[77] Convention on Cybercrime, Budapest, 23.XI.2001, available at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

The Cybercrime Convention in art. 1(a) of a computer system uses almost the same definition. Arguably, most RFID tags* meet this definition, since they are part of a system of RFID tags* and readers* that use software to process the data on the RFID tag*.[78] It may not even be necessary that the RFID tag* itself contains software, as long as it is part of a 'group of interconnected devices' that includes a computing devices (the reader*). Manipulating an RFID tag* therefore qualifies as illegal system interference (art. 3 Framework Decision), provided that it is not a 'minor' case, or as illegal data interference (art. 4 Framework Decision). Manipulating the more trivial RFID tags* would not be considered system interference, but it would constitute data interference.

If manipulating the RFID tag* would not in itself be criminal (for instance, because the tag does not qualify as an information system), it might still be illegal if it has certain consequences. For instance, if a price tag is manipulated so that an expensive dress is sold for a much lower price, the tag manipulation would normally be considered as fraud. Similarly, changing an identification tag that has an official registration function, for instance, of a dog or cow, could qualify as forgery. Here, much will depend on how strongly the law requires malicious intent or substantial damage; for instance, when two consumers swap loyalty cards containing RFID tags* to thwart Metro Futures Store's personalised profiling practice, or perhaps to gain more profitable offers, this can hardly be considered fraud for lack of criminal intent.

A final way in which RFID manipulation could be considered criminal is when it constitutes an illegal preparatory act. This may be the case in rare instances, for instance, when entry-card RFID tags* are manipulated to enter secured buildings where a terrorist attack is planned. Normally, however, the manipulation of an RFID tag* will not be sufficiently closely connected with a planned crime for it to be considered an illegal preparatory act.

Apart from manipulating RFID tags*, one can also eavesdrop on RFIDs. Intercepting the communication between an RFID tag* and a reader*, and unlawfully reading an RFID tag* will be a major area of concern. This, after all, is the core of the privacy concerns voiced by the public and civil society: people feel threatened when RFID tags* on bought objects can be read in shops (after the sale) or on the street. It is also a major issue in passports with RFID chips to prevent them from being read without right.

Intercepting the regular communication between an RFID tag* and an RFID reader* will be considered illegal interception in most legal systems. The Framework Decision does not have a provision on illegal interception, but the Cybercrime Convention in art. 3 criminalizes

[78] For Dutch law, Bart Schermer considers RFID tags to qualify as computers (Schermer, 2005: 83-84).

> *'the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.'*

Since the RFID reader*, if not the RFID tag* itself, is a computer system, intercepting the communication between these without right is illegal.

The same holds for accessing the data on an RFID tag* itself, for instance, by an unauthorised reader*. In this case, the data are not intercepted but illegally accessed. Both the Framework Decision (art. 2), at least for not-minor cases, and the Cybercrime Convention (art. 2) criminalise this. Both provide, however, that states may restrict the prohibition of illegal access to cases where a security measure was infringed. This implies that unprotected RFID tags* can, from the perspective of criminal law, be read by anyone even without right, and only RFID tags* with some security measure are protected by criminal law against unlawful access.

A final act against RFID that may have criminal implications is blocking the communication between RFID tags* and readers*, for example, by disturbing the electromagnetic radiation field. Such 'RFID blockers' are sometimes mentioned as potential measures to thwart privacy-threatening RFID readings. This may not as such be a criminal act, but in certain cases, it can qualify as illegal system interference ('the intentional serious hindering or interruption of the functioning of an information system,' art. 3 Framework Decision; likewise, art. 5 Cybercrime Convention), for instance, when a blocker is used to prevent all sales in a luxury-goods shop for several hours, or if animal-rights activists would systematically block the reading of cattle tags on a market.

4.3.2 Procedural criminal law

RFID will be used in criminal procedure in various ways. First, it may provide an interesting source of general intelligence, particularly if RFID is implemented on a large scale in an AmI world. The treasure-troves of data that may be collected and stored on the transfer of goods and persons and the relationships between objects and people could be data-mined by law enforcement to uncover activities of organised criminals or terrorist groups. Whether and to what extent such data-mining use of RFID data is allowed, depends to a large extent on the national legislation.

An issue that is likely to surface once RFID is widely embedded in society is a call for registration or retention of RFID data or RFID readings for law-enforcement or national-security purposes, similar to the current European legislation on mandatory retention of telecommunications traffic data.[79] Should RFID data provide a useful source of information

[79] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications

for law enforcement or intelligence agencies, which is not unlikely given their potential to provide systematic insight into a person's goods and travels if RFID data are combined, a debate may start about mandatory retention of RFID data. Similarly, governments could even mandate the tagging of all kinds of objects (cars, luxury goods, mobile phones, perhaps even children) so that they can be monitored more easily.[80] The political trend of recent years does not suggest that an 'RFID retention' debate is unlikely to arise. Such a measure would be highly questionable given the serious violation of the right to privacy (art. 8 European Convention on Human Rights) and other fundamental freedoms.

Second, RFID may become an interesting tool for criminal investigation of concrete crimes. The data of RFID tags* may be acquired by intercepting the communications between tags and readers*, for instance, to monitor whether a specific suspect with a known RFID tag* is entering a building. Most countries have laws allowing 'direct eavesdropping' or (in US terminology) 'oral interception', i.e., to intercept communications with technical means. Whether intercepting RFID communications falls within the scope of such provisions depends on the definition of communications; if a country restricts this to communications between persons, RFID interception will likely not be allowed on this basis. However, if the definition of communications is more liberal, e.g., exchange of data between entities, direct eavesdropping of RFID would be allowed. Alternatively, if an RFID system* qualifies as telecommunications – which might be the case in some jurisdictions – RFID interception can be based on the power to intercept telecommunications (art. 21 Cybercrime Convention).

The RFID data may also be acquired through accessing the tag itself. The RFID tag* could be searched or seized and subsequently analysed. The legal basis for reading an RFID tag* can thus be sought in the power of a search in general, or a computer search, if the RFID system* qualifies as a computer (art. 19 Cybercrime Convention). An interesting question is, if the RFID tag* does not qualify as a computer or information system, whether and under what conditions a search is allowed on the basis of the generic power to search. This will depend on the circumstances of the tag, for instance, whether it is located in a public space or in a private space, and whether it is tagged to an object or to a person. If the tag is implanted in a person, stronger conditions may apply because in that case, the interior of a body is being searched.

In case the investigation needs to be done covertly, search and seizure is not an attractive option. It is possible that the police needs to read RFID tags* on a suspect covertly. In that case, the investigation power of observation is likely to apply, again, under potentially different conditions depending on the circumstances and the specifics of the national legislation.

---

services or of public communications networks and amending Directive 2002/58/EC, *Official Journal* L105/54, 13.4.2006.

[80] 'The government could require equipment manufacturers to put serial numbers on every exposed surface so that the police would not need to move the equipment. Alternatively, the serial numbers could be stored in radio--frequency identification (RFID) chips that law enforcement could access with a sensing device.' (Tien, 2005: 882n.).

A third issue is the use of RFID as evidence. This seems fairly straightforward, as RFID can likely be easily fitted in the current mechanisms for allowing computer-related evidence. Most if not all countries allow computer data as evidence in court, and there is no reason to assume that RFID would be excluded on formal grounds as not fitting the allowed categories of evidence. A distinct issue is the evidential value that will be accorded to RFID. This depends very much on the kind of RFID tag* (how easy or difficult it is to manipulate it) and the procedures followed to secure the evidence.

A fourth issue relates to the use of RFID after the conviction, i.e., in the enforcement stage. Since RFID is a tracking tool, it might be used to keep track of prisoners or other convicts. Some countries might consider to implant chips in prisoners, or at least to tag prisoners' clothes or shoes. More immediately relevant might be the use of RFID to chips to monitor convicts on leave, to enforce court injunctions forbidding a person to appear in a certain area, or to enforce house arrest ('electronic detention').[81]

[81] RFID for electronic detention, often through ankle „cuffs", is already being used in, for example, the Netherlands (Miedema, F., Post, B., 2006), Austria (http://www.dergrossebruder.org/times/20060113153000.html), and Germany (http://www.iuscrim.mpg.de/info/aktuell/docs/Zwischenbericht.pdf).

5 Study of Social Aspects

5.1 Social implications and policy options for RFID and Profiling as AmI enabling technologies

Sabine Delaitre (IPTS)

5.1.1 Introduction

As we said in deliverable D7.3, profiling activities are essential to achieve the objectives of delivery of services in an AmI environment. Profiling activities require, use, and process data, which are related to a user's identity, his/her activities, characteristics, and preferences in specific contexts.

In general, profiling in AmI facilitates applications of interest to society enhancing social inclusion (cp. scenario 1, section 3.5), or enabling services making the everyday life easier (see Smart Home concept in D7.3). In addition, when it is applied on objects, profiling can help to fight against counterfeiting and fraudulent use, thus providing more security for the consumer. Moreover, a wide range of beneficial applications using RFID technology (Mullen, Moore, 2005), especially in the healthcare domain are announced by the private sector.

However, a series of social issues stem from profiling in AmI. The main issues are:

- **Loss of control**: The proliferation of automatically generated profiles could have a profound impact on a variety of decisions that influence the life of European citizens. At the same time, it seems unclear, whether and how a person could trace back (identify or determine) the sources of decision-making (answer to the question of when and what decisions are taken on the basis of such profiles).
- **Erosion of individual liberties**: Indeed, profiles can limit freedom of choice of users by confining them within the limited set of options on offer by the providers. Profiles tend to govern opaque decisions about individuals concerning their access to services, such as obtaining credit or a position.
- **Erosion of privacy - right balance between security and privacy**: In the context of AmI profiling may for example require some monitoring or surveillance of the users for the detection of physical activity. Monitoring and surveillance as well as other AmI-related technical solutions, procedures and business processes may erode privacy. Perhaps most people view privacy as a right that can be sacrificed, at least to some extent, if it leads to greater personal security.
- **Individual (personalised*) profiling vs. distributive* and non-distributive group* profiling (cp. D7.2, section 3)**: Individual and group profiling capacities have grown exponentially as a result of both the huge advances in technology and the increasing availability of readable data and traces, which can be processed and correlated.

- **Function creep:** The fact that technology and processes introduced for one purpose will be extended to other purposes, which were not discussed or agreed at the time of their implementation, is yet another important concern.

Thus, social issues related to privacy and security concerns arise, when profiling activity is carried out in an AmI environment. In this chapter, we will develop a part focused on privacy issues, a part focused on ethical issues and a part focused on societal issues, arising from RFID usage for AmI profiling. As explained in Chapter 2, RFID can be regarded as one instance of the technologies enabling profiling in AmI environment. So, all of the above mentioned issues also apply to RFID in a general manner. However, we will study to which extent these issues are applicable and what social implications may be expected of RFID usage, i.e., whether RFID technology may strengthen some issues and smoothen some others. In addition, we will explore the specific RFID related social implications so as to make a contribution to the debate on the likely benefits of RFID technologies to the European society.

5.1.2 Focus on RFID

Identified social implications will be described and organised around three topics: privacy, ethical and societal issues. Specific implications related to the respect for the individual, his/her identity, and personal data will be introduced, and societal issues related to more general implications on the information society will also be revealed.

5.1.2.1 Privacy issues

RFID tags* are potentially ubiquitous, almost invisible, may be embedded into or attached to objects without the knowledge of the individual that uses these objects; moreover, they can be read from a distance. However, regarding RFID related privacy threats, we have to distinguish two classes of RFID usage due to the diverse threats implied by their distinct uses, which are described below. The scenarios introduced in Chapter 3 are mentioned to show how they cover the different usages.

Fixed or handheld reader* with mobile tag

When the RFID tag* is embedded into clothes, items etc. and can be bought and carried by a user, the tag is mobile and the individual is named a tag-carrying user. In this class of RFID usage the reader* can be at a fixed location, such as at the entrance of the shop (see scenario 3) or mobile when it is embedded in a laptop (see scenario 2). Most of the privacy threats are considered in this context of usage.

Fixed tag with handheld reader*

The Korean Information Security Agency (KISA) exposes new applications using a mobile phone as an RFID reader*, in order to access new services (Lee et al., 2006). For example, each movie poster is equipped with an RFID tag*, which when read by the user may enable a ticket purchasing service. In this type of application, RFID tags*

are at fixed locations and the reader* is mobile and potentially identifies a reader*-carrying user. This kind of mobile service is defined as a Mobile RFID service (cp. especially scenario 1 for a description of this type of application). Additional privacy concerns may arise in this context, particularly due to the mobile aspect of the reader*. Such privacy issues are those stemming from mobile end-to-end data communications and wireless communications; for example privacy invasion due to the possibilities of sniffing, active intrusions (e.g. carried out by non-authorised reader* attacking the database or matching application) etc.

5.1.2.1.1 Personal privacy threats

In the article "*RFID privacy: an overview of problems and proposed solutions*" (Garfinkel et al., 2005), a list of personal privacy threats is described that mainly corresponds to the usage of RFID in the context of all that is outside the supply chain. This list of threats relates to the possible misuse of personal data as a result of the RFID tag* having a unique ID which can be associated to personal identity information. This list is composed of the following threats:

- Action threat, related to the individual's behaviour,
- Association threat, related to the customer's identity,
- Location threat, related to the tag location,
- Preference threat, related to the customer's preferences,
- Constellation threat; RFID network makes possible people tracking,
- Transaction threat makes possible to determine transactional information between users, and
- Breadcrumb threat, consequence of the association threat, related to personal information aggregation; this threat may lead to crime, or other malicious act.

From this list, almost all aspects of an individual's activity, the participation in everyday life (what you do, who you are, where you are and what you prefer) is threatened with disclosure. In addition, other threats appear by combination of the first ones due to the presence of network and information aggregation capacity in RFID systems*.

5.1.2.1.2 Societal privacy threats

Erosion of individual liberties

The main concern over the use of RFID technology in terms of data protection is that a lot of stored data needs to be transferred across different networks, organisations and stakeholders. The concern increases as information related to a variety of objects becomes linkable to the identity of their users thus adding data of a personal nature to the data that is being stored and exchanged. In addition, if such data is used to create profiles their use may limit the freedom of choice of users and lead to opaque decision making about individuals. It seems that RFID

may worsen the loss of liberties because of the silence[82] aspect. So, the likelihood becomes high that any action, such as participation in manifestations or rallies or strong preference for a specific brand, is collected and aggregated into a person's profile, usually without agreement. As a result and again without one's awareness or consent, some services may be denied with unpredictable consequences; for example one is denied a service because it is sponsored by a rival brand.

Function creep

As the RFID tag* becomes more commonplace through the deployment of diverse applications in many areas, so the possibility of 'function creep' increases. For example, embedded RFID tags* in casino chips designed to improve security against counterfeiting, could together with personal identifiers, be used to covertly track how people play each time they visit, recording stakes placed along with winnings and losses. Such RFID applications combined with profiling activities over which the user has no or limited control are considered by many to simply be an intrusion of privacy.

Another important aggravating factor stems more specially from the passive tag; indeed, this tag may exacerbate function creep in the temporal dimension because of its long operational life (about 10 years).

Surveillance

The wide use/adoption of RFID may lead to a new means of surveillance.[83] In this case, RFID is an additional instance of surveillance technologies, such as video cameras, access badges, the Internet, etc. However, RFID technology seems to arouse more reaction, compared with other technologies, because it seems that RFID use may strengthen surveillance misuse due to its power of information aggregation. Indeed, Locquenghein (2006) discusses about the possible emergence of a surveillance state through the use of RFID and the role of surveillance in a democratic society. After September 11, new policies move the nations towards an increasing need to secure and control, in order to combat terrorism. Consequently, some new processes could appear following the example of the *social sorting.*[84] So another question is to know, whether the integration of RFID in the current surveillance context will cause a new quality of surveillance in view of the possibility to combine different surveillance technologies and new consequences.

5.1.2.2 Ethical issues

This part will focus on specific ethical issues stemming from the misuse of data generated using profiling techniques, such as discrimination and victimisation, but also caused by possible but non acceptable uses of RFID implants to profile people.

---

[82] Silent aspect refers to the fact to not include the user in the decision-making process (no agreement) and the user is not aware of the communications among the components of RFID systems (reader, tag, and network).
[83] In the Article "Researching RFID's Surveillance Potential", the author M. Roberti describes the features that make RFID a potential tool of surveillance. http://www.rfidjournal.com/article/articleview/1765/1/1/
[84] Social sorting: Classifying and profiling groups of people in order to provide different services, conditions or treatment.

5.1.2.2.1 Discrimination

The misuse of profiling data by companies or other organisations may lead to discrimination of people according to their race/ethnicity or socio-economic status. RFID systems* have the potential to aggravate this threat, because of its capacity to allow the aggregation of a wide range of personal data. The omnipresence of such data may also make the common origins of stigmatisation (cultural, ethnic, socio-economic) more obvious and even generate new forms of discrimination. In that case, we can imagine a similar process like social sorting (Lyon, 2004), now based on RFID.

5.1.2.2.2 Victimisation

Citizens have a democratic right not to be treated as criminals in case they are not, otherwise, they will be unfairly victimised. Victimisation can be regarded as an AmI impact by describing a disproportionate reaction based on unfounded suspicions. Indeed, AmI technologies could jeopardise the presumption of innocence to the extent that decision-making is delegated to a computer, which interprets rules in a mechanical way, as black and white. Moreover, the possibility of wishing to maintain anonymity may be considered a suspicious reaction and may be perceived as out of the norm procedures. The victimisation threat may appear in the RFID profiling context not only because RFID is an instance of AmI technology, but also because RFID tags* are subject to malicious actions, so subsequent inadequate profiling is a real threat. Indeed, RFID tags* are vulnerable to viruses and worms,[85] and can be cloned. So, RFID worsens the victimisation threat because it gives attackers more options of modifying data and corrupting profiles. In addition, RFID cloning allows identity usurpation if RFID is used as a proof of identity; so an attacker may act under another identity or even sell cloned identities to criminals.

5.1.2.2.3 Special focus on RFID implants

Information and communication technology implants (ICT implants) in the human body have important ethical consequences particularly when these devices are accessible via digital networks. Subcutaneous RFID implants make people-tracking possible without the need for any correlation of profiling data or misuse of data. Consequently, this threat may cause a direct conflict with individual liberties. In addition, this threat may lead to non-authorised profiling because in this case the RFID implant can be used as an identifier of people.

The misuse of information then becomes easier and some ethically unacceptable instances (European Group on Ethics of Science and New Technologies, 2005) might be the following:

- ICT implants used as a basis for cyber-racism.
- ICT implants used for changing the identity, memory, self perception and perception of others.
- ICT implants used to enhance capabilities in order to dominate others.
- ICT implants used for coercion towards others who do not use such devices.

RFID implants are able to clearly encompass some of those adverse instances.

[85] http://www.rfidvirus.org/index.html, where this article by (Rieback et al., 2006) is available.

5.1.2.3 Societal issues

This part will introduce some societal issues generated by the implementation of new technologies, such as awareness and perception, adoption by the private sector, voluntary exclusion, or others stemming from profiling activities in AmI, such as loss of control. We will analyse how RFID influences those societal issues.

5.1.2.3.1 Awareness and perception

The public at large is not well informed as to RFID technology usage and consequences. The Capgemini report (2005) presented results on the awareness of consumers and only 18% of European consumers were aware of the existence of RFID tags* and applications. Public debates, workshops and consultations are being launched in order to diffuse correct information, deter false ideas (myths) on RFID technology and collect the opinion of the citizens. It is expected that awareness will be achieved only if even more efforts are implemented in view of the prospective challenges and opportunities for the European society out of wide-RFID deployment. However, the public debate is planned only through electronic means. There is a need to find a way to reach all potential users. An interesting way to involve citizens in the debate is participatory Technology Assessment (pTA), which integrates a learning process with a process of evaluation.[86] In section 5.2 a more detailed analysis of factors for social acceptance of RFID in retail will be presented.

5.1.2.3.2 Adoption by the private sector

RFID adoption by companies is a key factor of the current and future uses of RFID and directly impacts consumers. Indeed, it is also the responsibility of the industry to address customers' privacy issues. Consumers need to know how the enterprises, companies want to implement and put in practice RFID technology, what are their strategies and rationale. A wide adoption by the private sector may prove favourable to help establish industry specific privacy guidelines (Department of Commerce Washington D.C, 2005).

5.1.2.3.3 Voluntary exclusion: no longer an option

A radical measure in order for individuals to protect themselves is to voluntarily exclude themselves, i.e. by not participating in order to preserve their private sphere. This refusal to adopt new technologies or resistance to important changes is often caused by lack of trust or insufficient awareness of users for new technologies and their implications. However, in case of a wide RFID adoption, it would become difficult or even impossible to not participate, consequently not to be subject to any collection of personal data via RFID. In addition, as was repeated above failure to participate may imply some form of non-legal behaviour.

5.1.2.3.4 Loss of control

Decision support systems (DSS) (the decision is taken by the human) can be considered as convenience but when the user is excluded, the feeling of loss of control logically appears. In profiling as an enabling technique for AmI, the user is not directly involved in the decision making – only his/her preferences and information on his/her activities are taken into account – and this may lead to a feeling of loss of control above all when the decision does not fit the user's expectations. RFID technology may intensify the feeling of loss of control because of

[86] See e.g. one of the projects on RFID of the Dutch Rathenau Institute, at http://www.rathenau.nl/showpage.asp?steID=2&item=1347&searching=RFID.

its "silent" character (when the tags are read and which information is used) combined with its "invisible" character (which tags among a possible wide numbers of tags have been taken into consideration). These characteristics create problems for the user's awareness and understanding of the decision, consequently may cause the user to feel excluded in the decision making. For instance, in a Smart Home, a common example is the purchases based on the fridge contents, the preferences of the users, their activities and so on. RFID technology may be used, not only for checking the contents but also to monitor the users' activities. So, numerous RFID tags* may influence the decision. What type of purchases can I expect if I organise a party and each of participants brings special food (which I obviously need to put on my fridge), or what can I expect after having accepted to keep the children and the cat of my sister during the holidays?

5.1.2.4 Contribution to the debate

Privacy and security concerns arise when profiling activity is carried out. The main fears are related to the theft of personal data, related abuse, misuse, and 'silent' and 'invisible' surveillance; it is expected that suitable solutions will be implemented in order to protect the users against those threats. Considering the monitoring of private spaces (such as a bathroom) as a form of intrusive surveillance one could propose to forbid this. However, this type of monitoring might be beneficial for some users who, for medical purposes, require specific medical care. Therefore, it has to be up to the user to dictate preferences and requirements which any profiling application will have to respect.

It is preferable that solutions for appropriate usage of RFID should promote an 'opt-in' policy. Thus users will have to decide whether they want to participate and at which level they want to participate. Moreover, for any human decision making process, the users have to possess access to the information that enables decision making. This essential background information encompasses important requirements, such as:

- Transparency for the users' comprehension of the RFID usage context,
- Privacy options for the users' choice of their level of participation,
- Accessibility for the inclusive participation, awareness and learning of users, and
- Trust for the willingness of users' participation.

Achieving the above requirements is only one pillar of an "opt-in" policy. Indeed, in order to establish policies, technical aspects as well as legal and economic have to be studied. Therefore, some technical aspects are also described such as technical solutions or security options. So the following part will provide different key elements related to the above requirements, i.e. protection of the private sphere, accessibility and trust in order to open a discussion on how to achieve an "opt in" policy.

5.1.3 Protection of the Private sphere

In section 4.1.2 the legal framework of data protection has been analysed. This concerns the protection of *personal data*. As indicated some of the most challenging threats – dealt with in 5.1.2 – regard societal issues that result from the application of *group profiles* that allow for practically invisible but sophisticated social sorting. In this section the practical requirements that follow from the privacy threats discussed in section 5.1.2 are discussed. Many of these requirements were elaborated by experts, for example the so called "RFID bill of rights" published by S. Garfinkel in 2003.[87] Other requirements were developed by expert groups, including industry partners, for example the "Guide RFID and data protection" published in 2006 by the European Expert Group for IT-Security (EICAR)[88] or current EPC* standards (see Annex, chapter 8.4.2).

5.1.3.1 Transparency

A consumer has to be capable to evaluate the RFID usage context. And this implies transparency. For example, the users have to be aware how the RFID devices operate, understand the objective of any RFID system* and be represented by consumer protection organisations when RFID design decisions have to be made.

5.1.3.1.1 Right to Know

This policy concerns the fact that each individual has the right to be informed if a product contains an RFID tag*, what information is stored in the RFID tag*, when the tag is being read, with which type of reader*, where are the readers* positioned and so on. There have been calls for a mandatory label on any product equipped with an RFID tag*.[89]

5.1.3.1.2 Clarity of purpose

This refers to the need to clarify the purpose of any implementation of RFID-based systems. Therefore, the information contents, the storage and the use have to be defined in a clear way and the user has to be informed. This recommendation directly focuses on the prevention of function creep (cp. section 5.1.2.1.2).

5.1.3.1.3 Include the consumer's point of view in the RFID design decision

Important priorities for the consumers are to obtain the possibility and the conditions to freely choose the services in accordance with their needs and the protection of their interests. Designers have to take into account the position and point of view of the consumers represented by the consumer protection organisations.

Moreover, more trust in the system may be anticipated by associating consumers in the design decision loop.

[87] See http://www.technologyreview.com/read_article.aspx?id=12953&ch=infotech
[88] See http://www.eicar.org/rfid/infomaterial/RFID-Leitfaden-100406.pdf
[89] http://www.epic.org/privacy/rfid/

5.1.3.2 Privacy options

Interesting solutions should give the possibility to provide users with the means to select, among several privacy options, one option in accordance with their needs.

5.1.3.2.1 Spectrum of privacy options

So the first point is to determine a range of privacy options in accordance with the user needs but also those that the existing legal framework allows, and define each of the desired and allowed options.

Below, a first spectrum of privacy options provided by EPCglobal (Electronic Product Code* industry-lead standardisation):

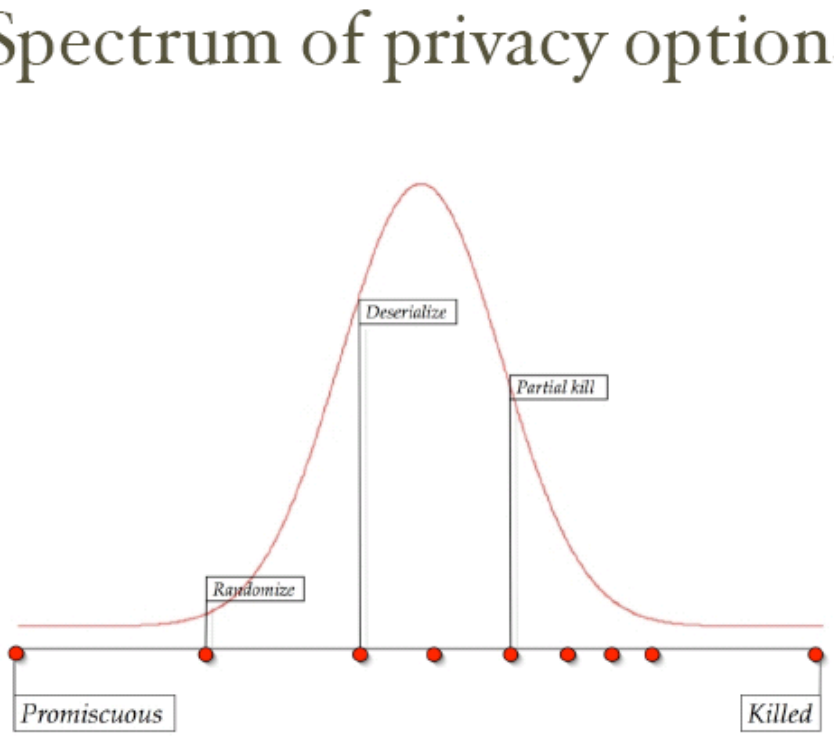

Figure 5: Spectrum of Privacy Options for RFID[90]

5.1.3.2.2 Technical solutions for privacy options

Technical solutions have to be provided to the user in order to give him/her the means to protect himself/herself and to choose the level of protection.

Herein, a brief introduction on the current mechanisms and a short analysis will show that from the existing mechanisms few provide a suitable way to combine user privacy and services. The related identified barriers are infrastructure issues, on-tag mechanism and opt-out policy.

[90] Source: EPC presentation, RFID Privacy conference, November 2003.

Some radical actions can disable the tag as the removal of tags (see CVS use case in Chapter 3), the clipping of tags (meaning that most of the antenna is removed, but tag remains active; patented by IBM) or by shielding the tag using a faraday cage. However, the two first actions imply that consumer has to be able to locate the tag (without mentioning the possible subsequent damage to the product) and the last one is not very practical for most common applications.

Killing: Some claim that a kill command is issued as soon as the tagged objects are purchased, in order to permanently deactivate the tags. This mechanism appears as a mean to protect user privacy. However, it is to the detriment of the benefit of post-sale value .

Recoding is the mechanism that enables the overwriting of the tag with a new ID number when this tag changes owner. So, recoding mechanisms require rewritable tags.

Killing and recoding mechanisms entail the installation of a reader*. Moreover, and as they imply a radical modification of the tag, the associated threat may be denial of service as a consequence of a non-authorised modification. In order to avoid this threat, additional infrastructure should be implemented. In addition, some studies are leading to the same conclusions: Even if the above infrastructure issues are solved, killing and recoding mechanisms do not address the problem of privacy (Molnar et al., 2005): Until the killing or the recoding, tags are readable – Therefore, one has to consider other options.

Sleeping seems a more suitable mechanism and should endeavour to conciliate privacy and services. Sleep/wake mode allows activating a deactivated tag. However, this mechanism is categorised in the on-tag (vs. off-tag) access control mechanism. On-tag access control mechanisms are located on the RFID tag*, although off-tag access control mechanisms put the access control mechanism on a device external to the RFID tag*. Consequently this mechanism implies a modification of the tag because the access control is in the tag itself and it is applicable only on high-cost tag.

So, the solution should focus on off-tag mechanism because *the access control doesn't require any extra complexity (hence, extra cost) on the RFID tag itself. Hence, off-tag access control has the advantage that it can protect low-cost RFID tags (like EPC tags)* (Rieback et al., 2005: 2).

Blocking: This mechanism is an off-tag access control mechanism. By creating a jammed area[91], a blocker tag[92] can make unreadable only the tags equipped with a privacy-control bit in the position "on". So, a blocker tag has no impact on tags whose privacy bit is off: general case for purchased tags. Blocking approach allows an all-or-nothing policy as to privacy protection, i.e. an *"opt-out" (vs. opt-in)* policy. So, blocking mechanism does not enable several levels of participation.

Soft-blocking (Juels, Brainard, 2004) is an approach promoting an opt-in policy because this approach allows revealing only a part of the data; so this approach could support a wider range of privacy policies.

[91] Technically this is done by intentional interferences
[92] Proposal by RSA laboratories and MIT. More details in the article (Juels, Rivest, and Szydlo, 2003: 103 -111).

5.1.3.3 Security options

Privacy invasion may be a consequence of unauthorised access. Security options that we describe below are considered as preventive actions in order to protect the private sphere.

If security is applied in order to guarantee the protection of the private sphere and it is completed, a subsequent benefit is to enhance the user trust and willingness as to the use of new technologies, like RFID.

5.1.3.3.1 Accountability

In this study accountability is used as a synonym of responsibility and liability. Accountability is a key concept for privacy-enhancing identity management. Therefore, transparency and accountability are necessary in order to respect the private sphere of the individual. Thus, it will be the basis of some safeguards against discrimination caused by the misuse/abuse/modification of personal data. For a detailed discussion of the liability issues that may arise and the adequacy of the present legal framework we refer to section 4.2 above.

5.1.3.3.2 Enhancing Information Security

Because one of the main components of a RFID system* is the network and the exchanged data is performed via networks, a need to foster the information security arises. This action will prevent the lack of co-ordination and co-operation in the field of network and information society may result in fragmentation of security policies in different states, heterogeneous application rules and solutions. There is an interest to encourage the knowledge exchange and co-operation between governments, industry and users concerned. This action will help to fight cybercrime in general but in particularly, the victimisation when it is subsequent to a criminal act. In addition aspects of multilateral security covering different participating service providers in RFID systems* and the users have to be dealt with (see chapter 2.5).

5.1.3.3.3 Technical solutions and regulations

Technical solutions and regulations (specification, protocol, etc.) have to be provided, in order to secure and guarantee the confidentiality and the integrity of the data when they are read, exchanged, or stored. Tag passwords, tag pseudonyms, and encryption are the proposed approaches,[93] in order to enable privacy protection in RFID usage contexts.

[93] Approaches described in (Garfinkel, 2005).

5.1.4 Other points to be taken into account

5.1.4.1 Accessibility

As we said, accessibility is required in order to support the inclusive participation (user acceptance), the awareness, and the learning of the users. Thus, this point may embrace different sub points, such as usability (vs. complexity) and training/education:

- **Usability** will promote system design according to a user-centric approach. Better usability will then support easy learning (i.e. learning by observation), user control and efficiency, thus increasing satisfaction and, consequently, user acceptance.
- **Training/Education** will promote education programs in order to learn how to use new technologies. Also it will increase the user awareness about the different possibilities and choices offered by RFID technologies and associated devices. This action is useful to increase the feeling of control and the awareness on the possible uses and consequences of the technology, thus in order to deter the misunderstanding on how the technology works.

5.1.4.2 Trust as a task force

Trust is necessary for any technology dealing with information related to user's identity and it is the basis of the users' willingness for their participation. Indeed, establishing public trust is a key point for any successful implementation. The trust concept encompasses different points, such as the user requirements, the trust model, the management of the trust and the solutions enabling trust. A trust model is the underpinning of any identity and access management system. The trust model establishes a verifiable and irrefutable process for managing user accounts, i.e. user profiles in the context of profiling activities. Trust models can be supported by contracts assuring information security for example via security service level agreements (SSLAs). However, trust also is a subjective concept because it is closely related to the perception of the risks and the benefits.

Regarding RFID technology, secure exchanges in view of authentication and confidentiality (trust criteria) have to be built in the different types of communication involved in a RFID system* – for example:

- Tag to reader*
- Reader* to tag
- Reader* to network

The different proposed steps (Natarajan et al., 2005) are the authentication of the reader* or of the tag and the encryption of the exchanged data between the tag and the reader* after the authentication process. The reader* connects to a server that stores all information of the tag, such as secret keys, etc.

The solution "antenna-energy analysis" (Fishkin, Sumit, 2003) is one example of a technical solution, based on trust perception. The "trust" hypothesis is: The further away a reader* is, the more suspicious it is. Therefore by using antenna-energy analysis the distance between the

tag and the reader* is exploited in order to adjust the tag's response (related to the disclosure of the information level) depending on the reader's* distance. However, this solution works only if we assume that those readers* that are further away have a malicious intent.

5.1.5 Conclusion

As shown in this section, RFID benefits may be negated by numerous instances of accidental or intentional misuse of the different components of a RFID system* and associated databases. Moreover, there is a wide range of issues relating to privacy and personal well-being (societal and ethical issues).

Indeed, various issues related to pervasive security problems can lead to enlarged privacy violations committed by insiders and outsiders. Examples are the misuses of databases associated with RFID tag* information or remote surveillance, whenever tags are vulnerable (without security guarantee). In addition, testing indicates that even passive RFID tags* may be interrogated over far greater distances than originally anticipated as said in a recent article (Neumann, Weinstein, 2006) on "Risks of RFID" taking stock of RFID risks and implications.

It seems crucial that we engage in the difficult task of evaluating the circumstances and contexts within which RFID systems* should or should not be used, and the rights of individuals and organisations to control whether or not they will be subject to various uses of these systems.

The proposal is to foster the protection of the private sphere by enhancing transparency and by identifying appropriate privacy options and security options for an "opt-in" solution, to increase accessibility relating to new technology such as RFID and to improve trust perception.

5.2 Social acceptance of RFID in retail

Martin Meints (ICPP)

5.2.1 Introduction

Since the 1980s (for example Davis 1989) intensive research was carried out to understand the factors that influence the acceptance of new technologies by the user. Originally dealing with Information Technologies (IT) in general, in the 1990s the research focused on mobile technologies and services. Target of this research was the ability to optimise products and services and to lower barriers for their acceptance from the perspective of the users. As a result the following relevant technical and social factors for technology acceptance were identified (cf. among others Spiekermann 2005):

- **Perceived usefulness** influenced among others by
  - Social status of the user and his openness for new technologies
  - Perceived fun
  - Communicational element (interaction)
  - Perceived personal freedom
- **Ease of use** influenced among others by
  - Usability
  - Interoperability (technical, formal and informal)
  - The need for attention
- **Trust in the service provider** influenced among others by
  - Availability and quality of the service
  - Reputation of the service provider
  - Perceived fairness of the price
  - Non-intrusiveness of the service, privacy preservation and data security
  - Perceived control over devices, services and personal data (all steps of the processing of personal data)

5.2.2 Perceived Control

Günther and Spiekermann (2005) carried out a survey about RFID and its acceptance with 129 representatively chosen customers of the Metro Future Store. A film in two versions was used to show benefits and drawbacks of RFID including possibilities to handle drawbacks such as PETs*. Before and after the film was shown, the participants answered a number of questions.

The majority of the participants in the survey understood and accepted the benefits of RFID in consumer products, such as easier operation of returns and guarantee services without the need of a receipt of purchase. They felt well informed about possible (and in this case hypothetic) PETs* for RFID systems* such as password protection or agent technology and felt that these PETs* are easy to use. Nevertheless, 73% of the users supported permanent physical disabling of RFID tags* after the purchase. This indicates that perceived control within ambient intelligent environments is more than a sub-factor of the trust in the service provider – for these types of systems it is a relevant main factor.

Spiekermann (2005) also summarised the elements of perceived control and the link of perceived control with privacy in ubiquitous computing* environments, though in this area further research seems to be necessary. In fact, since the 1970s privacy has been defined by many authors as control, for example to access the self, the group one belongs to or personal data. Based on this understanding in their proposed technology acceptance model, Spiekermann and Rothensee (2005) understand privacy protection as an aspect of perceived control.

Psychologists discriminate three types of control (Averill 1973):

- ***Information control***; information and knowledge about a system and related processes makes user feel a certain kind of control to use the known processes and the system
- ***Behavioural control***; the knowledge that a system behaves different (and possibly reproducible different) when a user does so; the user has influence on the behaviour of the system
- ***Decision control (choice)***; the user has different options and is able to choose among them

A forth type of control developed in social science (self efficacy theory, Bandura 1989) is the ability of users to deal with new technologies. Users tend to transfer past experiences with at that time new technologies to a give situation. If they were for example successful in adopting new technologies in the past, they will likely be open for other new technologies and motivated to deal with them.

Another factor influencing perceived control is the possession of relevant parts of complex systems. For example possession (or the lack of possession) of a communicational device can potentially influence the strength of the user's reaction in either direction.

The different factors of influence may result in either of two different tendencies:

- Positive reaction, i.e. technology acceptance
- Negative reaction, i.e. technology avoidance or stronger: opposition

In the end these tendencies are balanced out to a resulting decision with respect to technology acceptance or avoidance/opposition by the user.

5.2.3 The modified Technology Acceptance Model

Based on the results of this research, Spiekermann and Rothensee (2005) suggested a modified technology acceptance model for ambient intelligent environments. In this model the reaction of the user with respect to ambient intelligent technologies is understood as a balancing process of different tendencies. The different factors and their influences on tendencies and the resulting decision are summarised in the following figure:

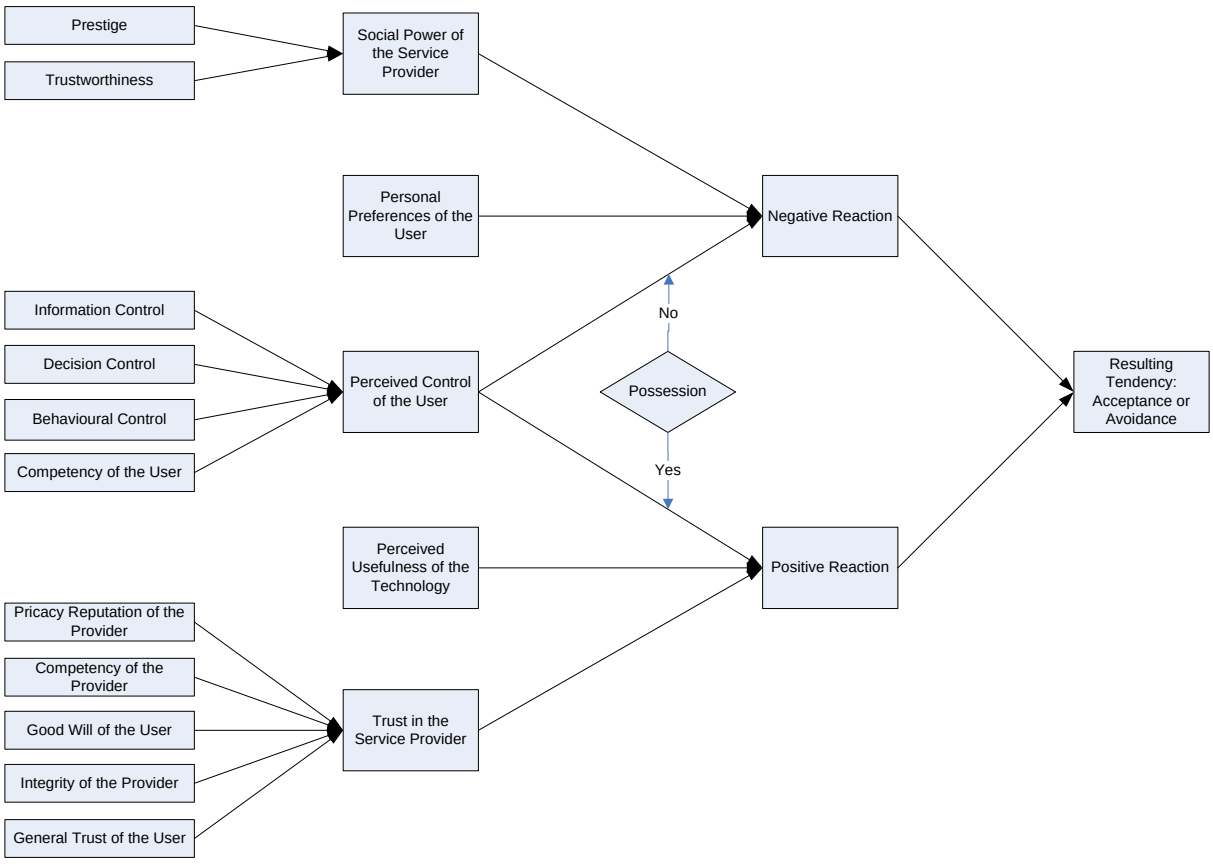

Figure 6: Factors for acceptance of ambient intelligent systems

Currently further research is being carried out by Spiekermann et al. ,which is focused on:

- The relevancy of the described factors

- The role of protection of privacy in perceived control

5.2.4 Conclusion

In this chapter factors for the acceptance of ambient intelligent technologies are summarised and investigated. In comparison with established technologies such as Information Technology (IT) including mobile technologies and services, for AmI-systems the perceived control seems to be of higher importance. Perceived control in the technology acceptance model suggested by Spiekermann and Rothensee includes informational self determination and privacy.

The proposed model describes that especially in cases where technology allows for a different design (for example in solutions based on RFID), ambient intelligent systems should foresee a sufficient control by the user to be able to enter the market successfully. System designs that do not take this into account will likely face opposition by the potential users or will be avoided.

Currently, there seems to be not much research with respect to technology acceptance for AmI technologies, apart from the presented approach. Research carried out so far seems to deal with specific aspects of user acceptance so far, such as acceptance of profiling in AmI environments (Bohn et al., 2004) or potential social drawbacks (Friedewald, Da Costa, 2003).[94] From this perspective the presented research proposes a technology acceptance model that connects well to established technology acceptance models for example developed by Davis (1989).

The proposed technology acceptance model still has potential for further development. Some of the introduced factors for example “Good Will of the User” or “General Trust of the User” currently seems to be explained quite generally. In addition the relevancy of the introduced factors is not fully assessed yet.

Currently further research based on a survey together with the newspaper “Die Zeit” and the German Federal Ministry for Economics and Labour is being carried out by Spiekermann et al,[95] with the target to describe the relevancy of the described factors more precise and to optimise the proposed model.

[94] Based on an internet search carried out on 16th of may 2006.
[95] See http://www.zeit.de/2005/45/Interv_Spiekermann, accessed on 16th of May 2006

5.3 Social Studies of Technology: Perspectives for AmI and RFID

Els Soenens, Mireille Hildebrandt (VUB)

5.3.1 Introduction

> *'The vision makes huge claims for the degree to which AmI is people-oriented. However, claims are typical for vision building (for example, the earlier Information Society vision of smart homes, and even the early 20th century mechanization of the household). They all promise to transform for the better the way we live, work, relax and enjoy ourselves. The AmI vision, however, specifically aims to avoid technological determinism. It recognizes the need for AmI to be driven by human rather than technological concerns. It proposes human-centred design and development guidelines together with other social concerns to advance this process. However, it remains to be seen if and how this manifesto will influence further research, development and design of AmI applications in order for the vision go beyond similar claims made in the past.'* (Punie, 2003:6)

Before presenting the major social theories that may be relevant for the study of technology in society, this section pays brief attention to the determinist perspective, as this may be a widespread perspective amongst both technology optimists and technology pessimists. Determinism, however, will not bring us much news about the way technologies evolve in continuous interaction with both other technologies and the people that use or design them. We will focus on a discussion of different social theories to capture promising ways to observe and describe socio-technical phenomena. Different social theories start from different assumptions when conceptualizing the relationship between society and technology. This results in diverging questions as to both the development and the application of RFID as an AmI enabling technology. Three constructivist perspectives will be presented: the social shaping of technologies (SST), the social construction of technologies (SCOT) and the actor network theory (ANT). While other social theories can of course be applied to the field of AmI, we think that the discrepancies between the technological determinist and social constructivist theories provide a good starting point to further elaborate the social study of AmI. In the next section (5.4), one of the more interesting types of constructivist perspectives, the TFI model, will be applied in more detail to RFID. As a conceptual framework TFI fits well the 'weak social constructivist' approach, discussed hereunder, since it explains how contextual factors (formal and informal) influence the technical layers of information systems (in this case AmI), without suggesting that the social layer of reality explains it all. In this section we will give some special attention to the ANT approach.

In the preceding section (5.2), a model for social acceptance of RFID is applied, tested and revised in the case of retail. The use of models may fit with mainstream sociological and psychological theory, rather than with social theory. The social theories discussed hereunder are not sociological theories. In the field of sociological theories, macro and micro sociological theories can be distinguished. Whereas macro sociologists study the society as a whole, micro sociologists study the individuals inside a specific society. To give only one example, structuralism is a macro sociological perspective which focuses on how social facts,

which can emerge both from consensus (e.g. Functionalism of Emile Durkheim, 1858 – 1917) and from conflict (Structural Marxism of Louis Althusser, 1918 – 1990), shape the behaviour of individuals. Against this perspective, we find micro sociological perspectives, as for example, social interactionism (George Herbert Mead, 1863-1931), which rather focuses on how people give meaning to their environment through interactions (Brutsaert, 1995). Social theory, however, extends the scope of the research by introducing aspects from outside mainstream sociological theory that may be lost to the eye of a well-trained sociologist. Social theories can be considered as frameworks that help one to assess reality from a lateral point of view. In general, social theories are particularly suited for cross-disciplinary studies, since they may be are less inclined to take preconceived ideas about the relationship between human society and technological artifacts for granted.

5.3.2 Technological and economical deterministic perspectives

In the category of deterministic theories, technological determinists assume that technological innovations are the major force in the determination of social behaviour. 'ICT users' are perceived as 'passive receivers' of new ICT's, because technological determinists suppose there is logic of causality between the implementation of new ICT and human behaviour. (Gripenberg, 2005: 25). As such, they believe that they can predict social and organisational changes. Technological determinists believe that technological development has it own internal logic and they often believe it necessarily leads to perfection or doom, depending on whether they are techno-utopists or techno-pessimists. Considering the causality between technological change and social change, Bruce Bimber (Bimber, 1994: 79-100) distinguishes between different types of technological determinism, of which the 'nomological' approach is the most outspoken as it does not attribute any influence to cultural or social factors and assumes that all consequences are intended consequences, valid for all people.[96] Economic determinists (also called managerialists) stress 'return on investment' and managerial rationality as main reasons to create and implement new ICTs. (Gripenberg, 2005)

In studying the vision of Ambient Intelligence, technological and/or economical determinists would concentrate on:

- Which are the necessary technological innovations to enable AMI?
- Which are the technological challenges in key enabling technologies of AMI?
- Which are the economical advantages of AMI?
- Cost-benefit analysis of implementing technological innovations
- Research on the causality between changes in social and organizational behaviour.

[96] '**Normative accounts** believe 'technology is an important influence on history' but, 'only where societies attach cultural and political meaning to it' (Bimber, 1994: 81). '**Unintended consequences** accounts assume technology does change society, however they admit that 'the outcome is unpredictable and uncontrollable' (Bimber, 1994: 89). **Nomological accounts** make 'the strongest claim about social change, a claim tied directly to technology. (…) Society evolves along a fixed and predetermined path, regardless of human intervention' (Bimber, 1994: 89).

The deterministic perspective is often used rhetorically. An interesting example may be of EU commissioner V. Reding when she stated on March 27th 2006: 'Radio Frequency Identification Devices (RFID), which will soon replace bar codes in your supermarket, offer tremendous opportunities for business and society.' (eGov Monitor, 2006). Others, such as T. Boone, are not convinced that RFID will replace barcodes soon: 'Bar codes, however, will not disappear anytime soon. Not only are they less expensive than RFID tags, they are widely deployed with well-defined standards and operational processes.' (Boone, 2005) The RFID Journal agrees with Boone in that: "Bar codes are inexpensive and effective for certain tasks, but RFID and bar codes will coexist for many years." (RFID Journal). By stating that RFID will soon replace bar codes the implementation of this technology is presented as unavoidable and this suggestions may in itself influence further developments.

5.3.3 Constructivist theories

Constructivist theories emerged out of a critique of deterministic visions of the relationship between technology and human society. Social constructivists believe that the design and/or use of technologies is socially constructed or shaped. Strong constructivism feels that 'technical capacities are not fixed but indeterminate and open to interpretive flexibility, not only during conception, design and development, but also when in use'.(Howcroft, 2004). Weak social constructivists in contrast, accept that social (f)actors can not unlimitedly (re)shape the use and design of technologies. Constructivist realists, like Latour, reject social constructivism in as far as it reduces everything to 'the social' or in as far as it separates 'the social' as a kind of substance from the rest of the world.

Classical constructivist theories concentrate on how diverse groups in society give specific meaning to the various technologies they use. The organizational theory for example believes 'information technologies are produced and interpreted as cultural artifacts that may symbolise a variety of values, beliefs and assumptions.' (Robey, 1997: 217). Classical constructivist theories would concentrate e.g. on the acceptance of AmI and on learning processes of humans coping with AmI applications. In sum, they research the users after the technologies have been developed.

The theories discussed hereafter are the three major and well known theories in the domain of the social study of technologies. These constructivists all hold a more intertwined view on the relationship between humans and ICT than classical constructivist theory. Social Shaping of Technologies (STT) and the Social Construction of Technologies (SCOT) argue that the design and use of technologies are socially shaped and/or constructed and they remark that the social construction of the use and meaning of technology is related to its content (the technological design which bears social choices). In this sense, they are weak social constructivist theories. These theories can be labelled as socio-technical theories (Gripenberg, 2005). ANT stands apart in as far as it puts more emphasis on the nonhumans and refuses to reduce everything to 'the social'.

5.3.3.1 SST: Social shaping of technologies

The notion of 'social shaping of technologies' serves as an umbrella for many studies, which use slightly different models, conceptions and focus on different research domains. Nevertheless it is their common aim to open the 'black boxes' of technology. SST theorists suggest that 'technologies are socially shaped such that their resulting material form reflects the structural and political circumstances of their development. Therefore the social relations of production (the practices, assumptions, beliefs, language and other factors involved in its design and manufacture) are built into technology, which has consequences for subsequent deployment' (Howcroft, 2004: 337). MacKenzie and Wajcman (1985) are well-known representatives of the SST studies. They perceive 5 mechanisms, through which the social shapes the technology. These are (MacKenzie, Wajcman, 1985):

- Existing technologies and science,
- Economics,
- Social relations,
- The state, and
- Gender relations.

Questions which could be posed by SST:

- Which are the construction mechanisms in the European AMI realization?
- How can gender issues influence the realization of the AMI Vision?
- Which are the structural and political influences?

5.3.3.2 SCOT: Social construction of technologies

SCOT has been developed by Pinch T. and Bijker W.E. starting from the sociology of scientific knowledge (Pinch, Bijker, 1987). SCOT falls within the scope of Science and Technology Studies (STS). STS takes an interdisciplinary approach. SCOT theorists do separate the social from the technological and are mainly interested in the effect of the former on the latter. However, the concept of the 'technological frame' is used to show how society and technology are 'like a seamless web' (Bijker, 1997: 97).[97] Three aspects are central in SCOT. These are: 'interpretative flexibility', 'the relevant social groups' and finally 'stabilization and closure'.

1. Interpretative flexibility

[97] 'The Technological frame of a social group is shaped while an artifact, functioning as exemplar, further develops and stabilizes within that social group – the social impact side of the coin. But a technological frame in turn also determines (…) the design process within that social groups – the social shaping side of the coin': (Bijker, 1997: 98).

Interpretative flexibility refers to 'the scope for technological artefacts to be adapted and used in ways not envisaged by the developers' (STREP, 2005: 35).[98] Technological artifacts are socially constructed artifacts. 'The interpretative flexibility of an artifact can be demonstrated by showing how, for different social groups, the artifact presents itself as essentially different artifacts.' (Bijker, 1997: 76). This also means that, depending on the social groups and context the use, meaning and problems related to technological artifacts are specific.

For example, in the case of RFIDs, the initial standardisation of RFIDs potentially minimises the interpretative flexibility of the systems. However, one has to be aware that interpretative flexibility of standards is to some extent still possible in the implementation phase: 'standardization can be 'interpreted differently' (Pinch, Bijker, 1987).[99]

2. Relevant social groups

Technology does not only create different problems and solutions for different social groups. The interpretation of the technology is different among social groups. SCOT tries to find the relevant social groups by concentrating on their shared understanding and interpretation of technology and of the problems and solutions that come with it. As such, there seems to be a circular reasoning in SCOT.

3. Stabilization and closure

Closure happens when a specific social group accepts a specific technology as a solution to their specific problem. This is not seen as a linear one-dimensional process. Critique of SCOT relates to the 'difficulty in accounting for closure. The possibilities of 'interpretative flexibility' (i.e. of 'choice') seem endless.' (William, Edge, 1986).

Questions, which SCOT could pose in relation to AMI could be:

- Which are the relevant social groups (who are the people sharing the same opinions and interpretations on AmI)?

[98] 'This incorporeality creates the scope for standards to be used in innovative ways during implementation. The use of this flexibility during implementation is a major element of standards dynamics, placing the use of standards out with the control of the actors maintaining and publishing them. Standards rarely exist in hermetic isolation and may be combined by users to create innovative constellations.' (STREP, 2005: 35).

[99] In this context one has to be aware that we know at least two different type of standards: (a) standards that follow a "good practice" approach such as ISO 27001, ISO 9000 etc. and (b) technical standards such as ISO 14443 and many others issued by different standardisation organisations.
Standards following a "good practice" approach typically include process models for e.g. information security management or quality management. The suggested models are not intended to be implemented one by one within an organisation, but they have to be adapted to the specific structures and needs of an individual organisation. They are meant to be used in a flexible way.
Technical standards describe on a certain technical layer (for example using the ISO/OSI layer model or specific system architecture models) how data transfer and processing has to be done. This always implies that there are other technical layers outside the scope of the standards, where different implementations of the standard can be used to do semantically very different things. A very obvious example for this is the internet service hypertext mark-up language (http). Originally developed to transfer hypertext pages only, today it is used to execute client server programs using various extensions within the original framework of http.

- How do we perceive the interpretive flexibility in AmI – do we perceive multimodal use?
- What is the interpretative flexibility of RFID standards in the implementation phase for a specific application?
- How did the process of closure take place?

5.3.3.3 ANT: The Actor –Network Theory

Like SCOT, ANT is usually categorised as part of Science and Technology Studies.[100] However, ANT theories hold a special position, because they reject the dichotomy of the social and the technical. Instead of thinking in terms of social and technical elements, they think in terms of humans and nonhumans that are perceived as actants in the field of technological developments.[101] ANT research focuses on a study of the way humans and nonhumans co-create hybrid networks, resulting in new artifacts. Also ANT does not differentiate a priori between micro and macro actors, because such qualification cannot be attributed until after the research has been performed and will depend on the context. As such, RFID enabled objects and locations are perceived as the result of the interactions between human and nonhuman actants that form complex hybrid networks. ATN would study the interaction between persons and specific ambient intelligent devices and spaces to find out exactly how they form or reconstitute new technological developments.

Within the scope of this deliverable we do not aim to present a detailed overview of ANT, however, we will point out some of the interesting ideas of ANT, as they could deliver interesting results if applied. For further introductions into ANT see the writings of Bruno Latour (Latour, 2005), John Law (Law, Hassard, 1999) and Michel Callon (Callon, 1991), who were the early developers of ANT. For a clear and relevant discussion of Latour's position Verbeek (2005, chapter 5) is a good source. We briefly discuss three of the central concepts of ANT: translation, inscription and irreversibility.

1.Translation

According to ANT design enables a **translation**. This means that the interests and objectives (of users and of the system) are translated by the technological artifact (the hardware and the software of the device). This is possible because the artifact contains a script, which 'includes programs of action for the users, and it defines roles to be played by users and the system.' (Monteiro, 1998: 9). Thus, technology 'becomes an actor imposing its inscribed program of action on its users' (Monteiro, 1998: 9). The script is inscribed into the materiality of the technology.

[100] Other theories, besides the SCOT and ANT which can be labeled as Science and Technology Studies are; the system theory of Hughes and the sociology of scientific knowledge. See e.g. (Bijker et al., 1987: 405).
[101] To Bruno Latour, networks are **not** technical networks. Here networks are not perceived as stable graphical representations of clear relationships and strategic positions. Instead, actor networks are assumed to point out to the actors/actans shaping actions.

2. Inscription

Other than SCOT, which adheres to a conception of interpretative flexibility, ANT introduces the notion of 'inscription' (See e.g. Hanseth and Monteiro, 1998). The concept of inscription implies that though technology is not considered static and fixed as technological determinists would have it, but also not endowed with unlimited flexibility, as some social constructivists seem to claim. Inscription stresses the dialectics in socio-technical environments, rather than dichotomies. For instance, Hanseth and Monteiro (1998) state that there is a link between the fact that a technology is designed for specific users and their ability to create interpretative flexibility. In other words; 'the closer the design of a technology is to its users, the stronger and more inflexible programs of actions can be inscribed into the technology and the more the technology imposes its inscribed program of action on its user.'(Gripenberg, 2005: 30). It seems to be the case that in such instances the inscription is more determinate of the interactions with the technology than in other cases, where the design is less user-specific. So, not all systems have the same strength of **inscription.** As a consequence, 'the inscribed patterns of use may not succeed because the actual use deviates from it' (Monteiro, 1998: 9). Precisely because ANT does not make an a priori distinction between micro and macro actants, it provides an interesting approach of 'shifting back between the 'designers' projected user and the 'real user' in order to describe this dynamic negotiation process of design (Akrich, 1992, 209)' (Monteiro, 1998: 13).

3. Irreversibility

Apart from translation and inscription, Callon's concept of '**irreversibility**' plays an important role in ANT. This concept can be compared to SCOT's concept of closure. Closure indicates the moment when the hybrid construction of a technological artifact is 'black-boxed', which means that we no longer look into the complex experiments that gave rise to its appearance but take it for granted as the specific technological artifact it has come to be. Irreversibility means stability and permanence. If we see the design phase of AmI enabling technologies as a phase that allows the construction of several (overlapping) actor-networks, irreversibility then means, that 'the translations between actor networks are made durable' showing 'how they can resist assaults from competing translations' (Callon, 1991: 159). In other words, when people with specific interests use the same technological solutions, irreversibility will be reached, which can be compared to what classical sociologists would call a 'process of institutionalization' (Monteiro,1998: 13) is reached. Because its detailed empirical interest in the construction of hybrid (human and nonhuman) networks, ANT methodology seems more apt to catch the workings of 'institutionalization' than SCOT and mainstream sociological theory.

An example of irreversibility could be the RFID tagging* of students (see also section 5.4.5). In Japan closure seems to have been reached whereas little or no people address privacy concerns over and against the security advantages. An increasing amount of institutions are tracking their children and students at school and on their ways to school. When looking at the stronger protests of students, parents and schools in Europa and the USA which have even lead to the withdrawal of RFID tracking trial programs, we can conclude that irreversibility of RFID tagging* of students (for the sake of security) has not been reached yet. ANT research would trace the interactions between the relevant actants in e.g. Japan, or in Europe, to

reconstruct the way such closure or irreversibility does or does not come about. Other than SCOT this process of reaching closure will not be reduced to 'the social', but investigated with a keen eye to all the relevant human and nonhuman actants.

Referring to Monteiro (1998), relevant aspects of ANT in the study of AmI are:

- 'Identification of explicit anticipations (or scenarios) of use held by the various actors during design'
- 'How these anticipations are translated and inscribed into the standards (that is the materials of the inscriptions)'
- 'Who inscribes them'
- 'Strength of these inscriptions, that is, the effort it takes to oppose or work around them'.

Based on section 3.7, we could apply the research questions of ANT to the scenario of CRM.

- The explicit scenario of use during design seems obvious: preventing fraud and providing easy stock overview.
- The anticipations are translated by the introduction of (item to item) RFIDs and follow- up possibilities of stock and sells.
- The inscription takes place in a process of product-developing between the human product developer and the material under construction.
- An example of the strength could be the fact that shop-owners now use the item to item RFID equipment to perform group profiling for the discovery of customer preferences and individual profiling techniques to target individual customers. This example may actually demonstrate that if the inscription allows for use beyond fraud prevention and stock overview a new hybrid network may evolve (of customer profiling) that may at some point reach irreversibility.

5.3.4 Conclusion

It is important to make explicit the theoretical underpinning of one's point of view, when doing research on the social implications of ambient intelligent environments. The answers to important policy questions can differ across the various perspectives. We opt not to take a deterministic stand of view on AmI. Especially we want to avoid determinist theories such as the 'nomological' theories discussed above. Nomological determinist theories stand in sharp contrast to ANT and social constructivist theories like the TFI model, since these nomological determinist theories cannot account for the crucial aspects of social context and human intervention in the development and implementation of AmI technologies like RFID. In order to create a holistic framework, ANT and other socio-technical theories can provide more enriched and detailed insights, especially with regard to the design and development phases of RFID and the 'Internet of Things'. In this section we have given some special attention to the possibilities of ANT, in the next section the FTI model will be explained and applied.

It should be interesting, if not highly recommended, to invest more into qualitative socio-technical research in the domain of ambient intelligence. The reason is that this could open

some of the – emerging - black boxes in the realization of the AmI vision as well as of the enabling technologies, allowing for effective intervention in an early stage of the road to 'everyware' (Greenfield, 2006, see section 2.1).

5.4 TFI perspectives on RFID as an AmI enabling technology

Ruth Halperin (LSE)

5.4.1 Introduction

This chapter seeks to offer an integrative outlook of some key issues arising in the context of RFID, AmI and Profiling. To this aim, a three-dimensional model called TFI is applied to map out current (and future) concerns associated with RFID as they relate to technical, formal and informal facets. In so doing, a more holistic understanding of the prevailing discourse on RFID is attempted, as well as a first step toward analyzing possible relationships between distinct disciplinary concerns.

The chapter is organised in four sections. First, the TFI model is briefly presented in the next section. The focus of each level of the model and its potential usefulness are highlighted. The following sections (5.4.2-5.4.5) discuss RFID systems* in relation to technical, formal and informal issues respectively. Finally, summary and conclusion are provided in section 5.4.5.

5.4.2 The TFI Model

In order to analyse the current issues associated with RFID systems*, it is helpful to have a conceptual framework as an aid to classification. Here, we employ the TFI model (Liebenau, Backhouse,1990; Backhouse, 1996) according to which information systems may be conceptualised and described as comprising technical (T), formal (F) and informal (I) layers. The power of the TFI model lies in its holistic approach to the study of information systems and related themes, so that the layer to which particular research pertains can easily be understood and its place within the field as a whole ascertained. The model can also be used to detect lacunæ in the current discourse and provide direction for future research and practice.

The technical, formal and informal layers of the TFI model when applied to information systems are defined as follows. The technical layer refers to the information technology component and its spheres of convergence, that is, hardware, software, data formats, protocols and so forth. The design of the technology such as the layout and appearance of the system are also facets of the technical layer. The formal layer of the information system refers to shared understanding of attributes and their formal structure. Policies, regulations and standards are typical manifestations of the formal. Finally, the informal layer refers to the ability to operate with attributes and context across domains. The informal layer of a system encompasses use or behaviour as well as systems of beliefs embodied in perceptions, expectations and culture.

The relationships between the abstracted layers of the TFI model are mutually constitutive and interdependent, suggesting that technical requires formal and formal requires informal.

Stamper et al. (2000) succinctly illustrate this interrelation of abstracted layers, explaining that:

> *informal* norms are fundamental, because *formal* norms can only operate by virtue of the informal norms needed to interpret them, while technical norms can play no role…unless embedded within a system of formal norms. (Stamper et al., 2000: 19).

Metaphorically, this can be viewed as a 'Russian doll' effect, where the informal is the outer shell containing the formal which, in turn, contains the technical. From the inside, the technical cannot be examined without first considering (unwrapping) the outer layers in turn (Backhouse, 2005: 16). Figure 7 below illustrates the interrelationships between the TFI layers.

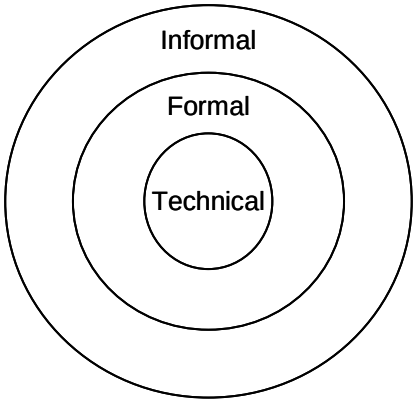

Figure 7: TFI-modell, adapted from Stamper et al. (2000: 19)

5.4.3 RFID - Technical Concerns

As discussed earlier in chapter two - RFID, although not a new technology, is by no means mature and various technical deficiencies are still evident in its current state of development. In technical terms, it is difficult to speak of RFID unambiguously as these systems differ on several important characteristics, such as frequency bands, transmission ranges, storing technologies, and means of power supply. Thus, the overall capability of an RFID system* will depend on each of these factors.

The technical diversity of RFID systems* also results in different procedures for authentication (e.g. none at all for EPC* tags or passive authentication for RFID in the context of machine readable travel documents) and codification (e.g., encryption of data) in the context of RFID security systems (Loncquenghien, 2006). Indeed, *security* arises as a major concern in the context of RFID. Security issues in RFID systems* pertain to availability as well as to problems of interoperation among distributed systems as elaborated in chapter 2.4 of this report. In addition, recent studies have demonstrated that RFID systems* are as vulnerable to destructive software viruses infiltrated using RFID tags*. One reason for the vulnerability of RFID systems* is given by Peter Neumann, a computer scientist at ISR

International. He commented that 'it shouldn't surprise you that a system designed to be manufactured as cheaply as possible is also designed with no security constraint whatsoever'.[102]

Further technical difficulties are associated with the *implementation* of RFID. As Eckfeldt (2005: 77) puts it 'implementing an RFID-based system is as much an art as a science'. Unlike other technologies, with RFID, significant gaps become apparent, between what is achieved in the lab and out side of it. For example, antennas that are effective in the lab can fail miserably when deployed in the real world due to unforeseen radio-frequency interference.

5.4.4 Formal dimensions in the discourse of RFID

Within the TFI model, formal issues typically refer to legal and regulatory matters that systems developers and managers must adhere to. In the current discourse of RFID, the development of formal criteria for protection of the *private sphere* arises as the key concern. The risks associated with RFID, against which policy and legal measures ought to protect are wide-ranging. In some views, RFID applications are seen as extremely risky, posing threats of privacy invasion, identity theft as well as bodily harm from stray radio signals (e.g., www.spychips.com). Others contend that RFID, when viewed in the context of similar technologies (LBS, GPS), do not offer anything that has not been possible so far except that RFID cannot be switched off voluntarily. Thus, the private sphere can also be violated in similar ways by other technologies. Between these two extremes, the more commonly accepted view seems to suggest that RFID pose a significant threat when data protection is concerned. As shown in chapter 2.3 this easily is the case, when no reliable measure are taken to cut the link between RFID tags* and physical persons. Introduction of new laws is being considered by different nation states and the EU. According to Eckfeldt (2005) several US states including California and Massachusetts are considering whether to implement RFID-specific privacy policy.

Locquenghien (2006) points out that the use of RFID might result in conflicts with existing data protection regulations and show that the criteria which should guarantee the protection for the private sphere can all be easily violated because of the technology's invisibility. It is concluded that data protection law is by no means prepared for the development of omnipresent data processing.

5.4.5 The Informal layer of RFID systems* – Analysis of User Perceptions

Informal questions refer to social and cultural norms that impact on whether the consumer/citizen will actually use the systems or whether there will be 'civil disobedience' or 'digital-refusenik' syndromes. While it is still early days for making generalised claims about actual behaviour, some indications as to norms and perceptions surrounding RFID technology may be identified. More specifically, three 'profiles' of RFID users arise from the literature. In some of the accounts, users are portrayed as ignorant about RFID and its associated risks.

[102] http://www.acm.org/pubs/cacm/newstrack/2006/embeddedrisks.html

In other cases, users seem to be knowledgeable (at least aware) of the technology but less so about the risks, largely perceiving RFID as harmless, a 'nice to have' technology, enabler of gadgets. Finally, potential users of RFID are described as knowledgeable about the technology as well as its risks (primarily invasion of privacy), and as actors who are making rational decisions for or against the technology based on cost-effectiveness considerations.

Lack of awareness among potential users of RFID is documented in a recent survey of the European Consumer reported in Capgemini (2005). An extreme case of such unawareness applies to the population of young children when RFID is used for the surveillance of school children as reported in Japan (Locquenghien, 2006). Unawareness, or rather helplessness, would also be the case of tagged hospital patients fighting for their lives rather than their privacy, presumably having little ability of becoming knowledgeable about threats of the technology in their vulnerable state.

With low awareness at the core of users' perception, RFID can be seen to 'creep' and pervade everyday life continually and *unnoticed* by many people. If this is the case (and so it will remain) then pervasive implementation of RFID is not expected to meet user resistance. It should not prove difficult to implement unless legal measures at the formal level are playing a role in regulating its terms of use.

Looking at users response to some of the current applications of RFID, such as access control in many holiday regions (Locquenghien, 2006), RFID technology appears to be harmless, perceived as a 'nice to have' technology that is associated with convenience and gadgets. In some applications of this kind, tags are attached to objects such as hotel keys and ski passes. In other cases, as in the Baja Beach Club in Barcelona, Spain, guests are offered a small implantable cylinder chip to identify them and which they use, in turn, to pay for food and drinks (Gossett, 2004).

A 'cost-benefit' approach prevails in the discussion of users' acceptance, appropriation or resistance to RFID systems*. This has been further described in chapter 5.2. In addition to the research summarised there Eckfeldt (2005) explores the prospect of RFID acceptance from a consumer point of view. Adopting a rational approach, he argues that as long as retailers/businesses maintain focus on their own agenda, consumers will reject the technology and resist its implementation. However, positive perceptions and acceptance can be achieved if consumers 'enter the equation' and businesses succeed in showing and creating benefits for the consumer. Eckfeldt (2005) thus concludes that the difference between successful and shunned RFID applications turns on delivery of clear, tangible value to the average consumer. Successful applications, he argues, overcompensate for whatever privacy fears they may involve. Consumers accept the risk of being tracked and their activities being monitored if they feel it is worth the benefits the application provides.

Angel and Kiztman (2005), discussing the relationship between RFID and cash, point to the severe threats posed on anonymity. They explain how the introduction of tags into bank notes (implementation also being considered by EU, (Ingdahl, 2004)) will serve taxation authorities thereby increasing control exercised by the state over the individual citizen, whether good or

bad. Notwithstanding this, objections are not being voiced because 'the message going out is that the benefits far outweigh the hazards in a marketing blitz aimed at gaining widespread public acceptance' (p. 6).

5.4.6 Summary and Conclusion

This chapter sought to offer an integrative outlook of prevailing issues arising in the context of RFID, AmI and Profiling. The TFI model was applied to map out current (and future) concerns associated with RFID as they relate to technical, formal and informal facets. Of the technical concerns in RFID systems*, security stands out as a key issue, with availability and interoperability being crucial to resolve. Technical difficulties associated with implementing RFID were brought fourth, owing to the significant gap between what may be achieved with the technology in a lab and outside of it. Formal issues were seen to embody concerns of legal nature, leading to the conclusion that the existing formal framework falls short at protecting privacy in the context of omnipresent data processing. Finally, analysis of the informal dimension in the context of RFID focused on emerging perceptions surrounding RFID technology. Three 'profiles' of RFID users were identified in the literature, namely, users portrayed as ignorant about RFID and its associated risks, users who seem to be knowledgeable (at least aware) of the technology but less so about the risks, and, finally, potential users of RFID who are described as knowledgeable about the technology as well as its risks (primarily invasion of privacy), and as actors who are making rational decisions for or against the technology based on cost-effectiveness considerations.

6 Implications for democracy and rule of law

6.1 Introduction

In this section we will assess some of the social implications that have been detected above, in terms of their possible effects on democracy and rule of law. We will base this assessment on the findings of FIDIS deliverable 7.4.

6.2 The framework of democracy and rule of law

6.2.1 Self-identity, democracy and rule of law

In deliverable 7.4 we made a first assessment of the potential impact of profiling on the identity of the European citizen. Self identity is crucial for both democracy and rule of law. Democracy presumes the participation and/or representation of empowered citizens, with a balanced sense of self. Rule of law presumes legal subjectivity, as this creates the framework for citizens to take their position in the network of private and public relationships. As legal subjects citizens can claim their rights and be held accountable for the obligations they have been attributed. If any type of technological practice diminishes the preconditions for such legal subjectivity we should reconsider its implementation. In D7.4 we claimed that privacy is not only a matter of personal well-being or private expectations, but first of all a public good that is the precondition for a society in which individual liberty (freedom from interference) and citizen's participation (freedom to engage in public and private enterprises) is celebrated. This means that privacy is not a commodity that can be exchanged for short term comforts, or arbitrarily traded for some personal gain. It also means that if people feel that they are in control, while in fact they are not aware of the consequences of their actions, the preconditions for individual liberty and responsible citizenship are not in order.

6.3 Profiling, self-identity and 'The Internet of Things'

6.3.1 Profiling and self-identity

The problem with profiling is that it infers knowledge from data and that even in the case of group profiling on the basis of anonymised data, the impact of the profiles can be quite impressive. In the case of anonymisation Data Protection legislation is not applicable, which means that a data subject has no means to find out about the profiles that may impact the risks and opportunities he or she is subject to. Profiling allows targeted servicing, fine tuned price-discrimination e.g. in insurance, or black-listing of categories of people in the field van criminal investigation and intelligence. The freedom to take part in private and public networks may increasingly be created or denied on the basis of inferred profiles, while at this moment citizens don't have the technological tools to screen which profiles have been applied to them, even if Data Protection legislation were applicable.

6.3.2 Autonomic profiling, AmI and self-identity

In an AmI environment the adaptive capacities of the environment depend on adequate profiling. The aim of AmI is to allow seamless and autonomic adjustments to consumer's inferred habits and desires. The aim is to anticipate these habits or wishes, which means that one does NOT provide a profile on the basis of what one thinks to be one's preferences, but that one trusts the system to infer them and to adjust the environment accordingly. Evidently, this seems to cause a loss of control, because the preferences are not deliberately articulated by the end-user. Referring to what has been written in the introduction to this deliverable (section 2.1) autonomic profiling aims to discharge us from deliberate reflection on seemingly trivial logistics, just like our autonomic nervous system does. We do not get upset because a change in heart rate has been decided upon without our consent, and likewise we should not complain that doors open before we have reached them and room temperature is tuned to our liking without deliberate manual input. However, the proliferation of data leaked, collected, stored and aggregated in an AmI environment, and the subsequent proliferation of profiles may have an impact beyond anticipative logistics.

This does not only depend on possible abuse of profiles, like use by a person or organisation that is not authorised to employ them, or use for an illegitimate objective (for which consent has not been given, or which is illegitimate of itself, like ethnic discrimination). More importantly, the focus should be on the extent to which it is (im)possible to detect whether or not profiles are abused, and whether or not a citizen can effectively counter such abuse. For this reason Data Protection legislation is first of all a tool of transparency, aiming to empower citizens to guard their liberty and freedom. To the extent that this transparency is a legal right but a technological impossibility the self-identity of citizens is at stake.

6.3.3 The Internet of Things: The end of constitutional democracy?

In recent years books have appeared announcing the death of privacy. The question mark behind this heading indicates that this section is not a funeral announcement for constitutional democracy. However, widespread introduction of RFID systems* beyond supply chain management may unintentionally provide an infrastructure with totalitarian overtones, which may be difficult to keep in check once implemented. Totalitarianism is equivalent with the death of the private sphere, due to pervasive colonisation by the state. The cliché of Big Brother has been referred to in order to alert citizens to the loss of their privacy, due to permanent spying by state authorities. Legal scholar Solove indicates that this metaphor should be complemented with another metaphor that more aptly discloses the unintentional rather than deliberate, the omnoptical rather than panoptical and the anonymous rather than personalised enforcement mechanisms that may emerge in the wake of an 'Internet of Things'. In *The Digital Person* Solove (2004) discusses Kafka's *The Trial* as a more adequate metaphor to describe the network of data controllers that hold our data and our profiles, trading them to the highest bidder and thus allowing ever more precise profiling of individual people.[103] The intention of these data controllers is not to target a particular person, nor to control an entire society. Their objective is more modest: to make a profit by tuning their

[103] Kafka's famous novel *The Trial* (Kafka, 1999) is about a person who is accused and tried without finding out what the accusation actually is, by a seemingly anonymous authority.

services to the inferred personalised preferences of as many customer as possible. However, the availability of such profiles will suit intelligence and criminal investigation as well as insurance companies and social security or health care institutions. If the 'Internet of Things' takes on, any data from one's past may be correlated at any time, anywhere, to produce a profile that allows the profiler to anticipate our actions, or our mental or physical state. The right to oblivion will be lost. Like Joseph K. in Kafka's *The Trial* we may become aware of the fact that anything we do may be used against us at some point in time and we may begin to normalise our actions in order to prevent future harassment. As indicated before, the point is not whether government authorities or insurance companies actually abuse profiles to trace and track us for illegitimate purposes, but whether we have the means to detect such abuse and to restrict access to our pastness. In legal terms one could paraphrase by asking the question to what extent we need a legal right to oblivion, to counter the emergence of detailed 'dossiers' (Solove, 2004) containing all the brute facts of our lives. Or, rephrasing in terms of narrative self-identity (Ricoeur, 1990; Hildebrandt, 2006): to what extent must a person be able to articulate the story of her life, in which these brute facts are placed in the context of a first person perspective, having decided what to forget and what to remember? It should be obvious that complete control over one's narrative identity is both impossible and undesirable, but at the same time it should also be obvious that a balance is needed that allows a person to reconstitute her identity without being judged entirely in terms of her machine-readable past.

Solove's analysis confronts one aspect of the implications for constitutional democracy: Fear of being charged with unknown accusations on the basis of (long) past machine-readable events, (physical or mental) states or interactions. Another unintentional consequence for a viable democracy is described by Cas Sunstein (2001) in his essay *Republic.com*. This is again not yet about abuse of profiles (who would not be against that), but about the impact of profiling on the identity and agency presumed by democratic representation and participation. Sunstein argues that democracy is based on an effective practice of free speech, for which he detects two distinctive requirements.

- First, he claims, 'people should be exposed to materials that they would not have chosen in advance. Unplanned, unanticipated encounters are central to democracy itself' (Sunstein, 2001:8).
- Second, he claims, 'many or most citizens should have a range of common experiences. Without shared experiences, a heterogeneous society will have a much more difficult time in addressing social problems' (Sunstein, 2001:9).

Sunstein discusses profiling in terms of filtering, especially 'collaborative filtering' (a type of group profiling) and 'personalised shopping' (based on a type of personalised profiling). While he acknowledges the advantages of the ensuing customisation, he also warns for the disturbing consequences: 'to encourage people to narrow their horizon, or to cater to their existing tastes rather than to form new ones' (Sunstain, 2001:26). Democracy should foster the unexpected to keep its citizens on the alert and provide room for change, and democracy should celebrate common experiences even if they don't all fit one's individual preferences. Like Solove, but from a different perspective Sunstein again describes the potentially totalizing effect of an 'Internet of Things' that caters to everyone's inferred preferences. Other than Solove he demonstrates that people are not being normalised under the pressure of fear for future incriminations, but – on the contrary – thanks to a totalising type of customisation. Before we have time to consider alternative choices the environment already caters to what it

infers from our past interactions. Living in a filtered environment may isolate us and may render us impotent in confrontation with the polluted space of unfiltered encounters. Deliberative democracy needs such unfiltered confrontations to get to the bottom of things, before deciding how to proceed.

6.4 Constitutional democracy in a tagged world

Do the warnings of Solove and Sunstein mean that we should abstain from further research and development of RFID systems*? Such a conclusion would certainly not fit Sunstein (2001). If we understand the precautionary principle as a principle that warrants further investigation in the case of uncertainties, not equating it with risk aversion or sitting back, then we may have to expand the exchange of information initiated at the Public Consultation by the EC, during March-June 2006 and invest in exploratory research into the impact of a tagged world on the capacity of individual citizens to freely participate in well-informed public and private deliberation.

This chapter does not provide ready made solutions to preconceived problems, like privacy and security (which does not mean that we should underestimate these problems). Taking the perspective of democracy and rule of law this chapter aims to provide a direction that should guide both the definition of the problems and their solutions. Otherwise we may end up like the drunken man who returned home late at night and dropped his key on the street. He kept circling the small piece of the street that was illuminated by a street lantern, without locating the key however. When a passer by inquired whether this was the place he lost the key he said: 'No, but this is the only place with enough light to see something like a key'. Better get a torch from somewhere and start looking elsewhere.

If privacy is a public good and a precondition for constitutional democracy we cannot reduce it to anonymity. The problems that may occur if we animate the things in our environment with RFID tags* that are interconnected via RFID-readers* and online databases will be the result of pervasive autonomic profiling. Anonymity will not counter the effects of such profiling. Those spying on us will be machines that will mainly be talking to other machines. They will not be interested in you as a person, but rather in you as a potential customer, offender or illegal immigrant. However, the profiles they generate will impact the chances you get in life, while you will be mostly unaware of what is going on. We must therefore invest in adequate ways to technologically enable people to access the knowledge that may be used to deal with them. We must not only minimise the transference of personal data, but also maximise the transparency of the subsequent data processing, whether anonymous or not. More importantly this transparency should concern both one's electronic footprint and the profiles that may be applied to us, even if these profiles were constructed without using our personal data. The next generation of PET's* may have to be TETs*: Transparency Enhancing Technologies, protecting our privacy – not just our personal data.[104]

[104] In the context of user controlled Identity Management Systems (type 3 IMS) history management is an already established privacy enhancing function. State of the art in history management recently was summarised by Meints (2006). History management uses basically data generated, received and transferred by the user of the IMS himself as source. For the evaluation of potential privacy impacts and the suggestion of options in the context of identity management by the user reporting functions are used. Extended reporting tools using data mining techniques have been discussed.
History management can be understood as a predecessor technology to the suggested TETs. In difference to

6.5 Conclusions

This means that the fair information principles of data protection legislation need to be reinterpreted or extended to cover the protection of individual persons against inclusion or exclusion on the basis of knowledge they are not aware of. The focus on protection of personal data does not cover the access to profiles inferred from anonymised data, nor does it provide the legal tools to contest the knowledge claims they contain. However, to have legal access and legal tools to contest invalid, irrelevant or unlawful use of profiles is useless if we do not have the technological infrastructure to enable this. The technological infrastructure that is being designed at this very moment to facilitate a fully operative AmI-environment must incorporate the technological means to allow adequate anticipation of the profiles that could be inferred from our behaviour. If the 'Internet of Things' turns our environment into an external autonomous nervous system, we may in fact need autonomic counter-profiling to give substance to our rights to oblivion, consent and contestation. This is what deliverables 7.8 and 9 should explore in more depth and detail.

TETs history management uses personal data of one data subject only combined with static or dynamic rules implemented in the reporting tool. As basic data for history management includes a fraction of the data the data controller is using only and business targets and mining methods of the data controller are not known, history management can be understood as a limited parallel profiling by the data subject.
Another important aspect of history management in the context of RFID is that most of the RFID systems used today do not allow for it, as due to the remote and unobserved readout of the RFID tags the data subject has no basic data to perform any history management. To implement TET's design of RFID systems has to be changed fundamentally compared to today's RFID systems.

7 Summary and Conclusions

Mireille Hildebrandt (VUB), Martin Meints (ICPP)

RFID is one of the enabling technologies for Ambient Intelligence and the 'Internet of Things'. It may provide us with a new experience of things and space, as the offline world goes online, connecting everything everywhere, turning Weiler's ubiquitous computing* into Greenfields 'everyware'. In itself a tagged environment only produces an unlimited amount of machine-readable data. To make sense of this profusion of information we will need techniques and technologies to filter and select what is relevant at a specific moment in a specific context. RFID can only turn a tagged environment into an adaptive or even intelligent environment with the use of profiling technologies. To achieve seamless real time adaptation on the basis of real time inferred profiles, we will need what has been called autonomic computing, which will restrict human intervention to a bare minimum. This evidently poses big questions around the feasibility of privacy and the capacity of data protection legislation and PET's* to provide such protection. If the 'Internet of Things' builds on pro-active computing, one of the challenges of the age of 'everyware' may be how to design a legal and technological framework for renewed interactive computing.

In this deliverable, the objective has been to provide a multidisciplinary description of the state of the art of RFID as an AmI enabling technology and to anticipate some of the scenarios that could develop if the technology takes on.

In Chapter 2, after outlining the relationship between RFID, profiling and the 'Internet of Things', the report starts with a technological description to explain how - from a technical perspective - RFID systems* can be understood as forerunners of AmI systems. They share to a large extent the infrastructure that is also needed for profiling purposes – and in fact early prototypes combining RFID, AmI and profiling have already been tested. This integration is clearly economically motivated: Why not use an already installed infrastructure for RFID systems* to add additional functionality such as early AmI (adaptive displays), why not use already collected data for profiling purposes?

In the three case studies of Chapter 3 different business targets for the introduction of RFID, characteristics and existing problems of the technical implementation, relevant legal grounds that were taken into consideration and privacy aspects have been described. Among these case studies in particular the Metro Future Store is remarkable, as it shows characteristics of AmI environments and uses profiling techniques. In all case studies a centralised management of security and privacy is possible, though along supply chains privacy and security have to be enforced based on appropriate contracts.

In the three scenarios of Chapter 3 aspects are highlighted that need to be taken into consideration when RFID systems* become an integral part of AmI environments. In this case an infrastructure controlled by one enterprise and thus suitable for a centralised management of security and privacy is transferred to an open accessible infrastructure with the need of a decentralised, multilateral management of security and privacy. This situation can be compared to the internet we know today. In the scenarios different threats typical for such infrastructures, like e.g. as technical failure of RFID systems*, intended attacks leading to loss of confidentiality of data processed and multiple use of collected data are described with their potential consequences for users.

Based on the use cases and the scenarios three legal aspects are analysed in Chapter 4:

(1) The applicability of the European data protection framework,

(2) Liability issues caused by RFID and,

(3) Implications of RFID for criminal law.

As long as data are not anonymised, data collected from RFID in AmI environments can be used directly or indirectly to identify a person – in which case the European data protection framework applies. However, in complex RFID systems* it can be difficult to determine from the user's (or data subject's) perspective who is the data controller and thus responsible for the implementation of data protection and security. In most of today's examples (see use cases) this is the 'tag deployer'. The possibility to deploy and read RFID tags* without the data subject's awareness is an inherent problem of RFID technology; the respective use of RFID in the Metro Future Store use case is clearly unlawful. Among others, the application of proper user information and clearly visible signs to indicate that RFID tags* and readers* are in place or used, may help to solve this problem. In general we have to expect three trends with respect to data protection and RFID in AmI environments:

- All tagged objects become a collector of personal data,
- The 'presence' of these smart objects as well as individuals who carry them is characterised by its 'always on' nature, and
- The resulting cascade of data continuously feeds an enormous amount of stored data.

Besides that, data protection seems to restrict itself to the protection of personal data, while in an environment that depends on autonomous profiling we need to focus on protection against the automated application of profiles that we are not aware of. Though one has a legal right to contest automated decisions based on automated profiles, this right seems ineffective as long as the technological infrastructure does not provide access to the profiles that may impact our lives.

Liability issues of RFID systems* in AmI environments have already been analysed with respect to violation of data protection legislation in the SWAMI project.[105] But in addition to this aspect liability caused in a different way and by other reasons such as technical failure or deliberate attack has to be taken into account. In addition to potential difficulties to address liability issues properly (who is liable for what damage caused how?) there is no generally unified European legislation on contractual and non-contractual liability, apart from partial common grounds set up by Directives such as the Directive on Defective Products (99/34/EC). Service providers and users depend on national law. Approaches to harmonise legislation so far have not been successful.

In the context of liability the 'always on' nature of RFID tags* raises a number of questions with respect to liability. Questions of interest for future legislation in the context of liability are for example:

- Should there be a right to withdraw from the RFID system* and to switch off RFID tags*?

[105] See http://swami.jrc.es

- Should the mere 'participation' in AmI environments using RFID already be interpreted as 'consent' by the users or customers of the services for processing of any kinds of personal data?

The implications of RFID for criminal law are largely unexplored. In this context, areas of interest are:

- The manipulation of RFID tags* and systems in different ways, where in most cases existing legislation - for example based on the Cybercrime Convention - can be applied
- The use of RFID as a tool to facilitate (already defined) crime such as stalking, fraud, theft etc.
- The use of RFID to prevent crime such as forgery or theft
- The use of RFID in criminal procedure such as
    - Use of RFID and AmI-systems as a source of general intelligence
    - Use of RFID for specific criminal investigations
    - Use of RFID as evidence
    - Use of RFID in the enforcement stage after conviction

With respect to liability issues European harmonisation of legislation is needed. As many questions in the legal context of RFID are still open, further research is needed with respect to:

- Implementation and enforcement of data protection legislation
- Giving and withdrawing consent in the context of liability and
- The use of RFID in criminal procedure

Chapter 5 starts with an overview of the social aspects. The most relevant issues are introduced and discussed as follows:

- Discrimination, exclusion and victimisation as consequences of inadequate profiling
- Loss of control by the user
- Erosion of individual liberties
- Erosion of privacy
- Shift in knowledge as a consequence of the use of profiling technologies
- Function creep of already introduced RFID systems* can increase these issues

To develop an acceptable way to using RFID in AmI environments it is argued that a public debate is needed. Relevant aspects of this debate could be:

(1) Transparency for users / citizens on the usage of RFID,

(2) Privacy options for different levels of participation of users in RFID and AmI systems,

(3) Accessibility of an inclusive and well informed participation, and

(4) Appropriate trust models from both the perspective of users and operators of the systems.

Several concrete measures have been suggested at the social as well as the technical level to achieve a balanced result in this debate.

The next section of Chapter 5 provides a more detailed account of social acceptance, by the use of a technology acceptance model that is applied, tested and revised in relation to RFID and profiling in the context of retail. Technology acceptance models target at the optimisation of products and services and to detect and lower barriers for their acceptance from the perspective of the users. Since the 1980s technology acceptance models have been applied for IT in general, mobile technologies and services and lately also RFID in the context of AmI environments. In addition to established key factors for the acceptance of new technologies in general such as (1) perceived usefulness, (2) perceived ease of use and (3) trust in the product or service provider, *perceived control* seems to play an important role for RFID in AmI environments. Important elements from the perspective of the users that can be influenced by service providers are:

- To be informed and to have knowledge about the system (information control)
- The knowledge that his behaviour changes the (re-)action of the system (behavioural control) and
- To have different options (choices) to interact with the system (decision control)

Taking these aspects into account when designing AmI systems, the resulting solutions will likely have an increased user acceptance and thus promote diffusion of RFID into the market.

In the following section of Chapter 5 a set of social theories is discussed to provide a better understanding of the study of interactions of society with new technologies. In general one can discriminate two ways of looking at the relationship between technology and society:

- Technological and economic deterministic theories assuming that new technologies or economic rationality determine social behaviours and
- Constructivist theories assuming that the design and use of technologies is always a construction.

While some – social - constructivist theories seem to reduce technological development to social developments, others take note of the complex interactions between the human and the nonhuman players in the field, attributing actions to nonhuman actants without falling prey to the determinist perspective. Special attention is given to Actor Network Theory (ANT), which allows a pertinent insight in the way specific technologies meditate the way we act, by inducing certain kinds of behaviour and inhibiting others. ANT research can trace the way in which technologies are in fact constructed as a result of the continuous interaction of human and nonhuman actants. In the case of an emerging 'Internet of Things' it is thought to be particularly important to trace the development of such construction, in order to allow adequate assessment at an early stage. Such assessment and subsequent action should take place, before a technological infrastructure settles down that renders empowerment of citizens

virtually impossible, because they do not have the technological and legal means to access and contest the knowledge that interconnected THINGS have of them.

In the next section the so called TFI model is presented, which discriminates three layers of systems: the technical, formal and informal layer. These layers can be used to categorise relevant aspects of RFID in AmI environments and to identify potential areas of action. Relevant aspects as a result of this analysis are:

- On the technical layer:
  - Security, compatibility and the gap between laboratory and practical implementations of RFID
- On the formal layer:
  - Aspects of addressing and implementation of legislation especially in the context of data protection
- On the informal layer:
  - Analysis of groups of potential users shows at least at two of them a significant awareness and information deficit with respect to chances and risks of RFID.

Finally, in Chapter 6, the implications for democracy and rule of law have been explored in reference to deliverable 7.4. First of all it is established that a viable constitutional democracy both presumes and produces empowered citizens that have an adequate sense of being in control of their own lives. As has been explained in D7.4, in the context of democracy and rule of law privacy is a public good that needs to be protected to safeguard the central tenets of democracy. If widespread, ubiquitous and autonomous profiling proliferates - as it must in the case of AmI - we need to reinvent the legal and technological tools for transparency (of those in power) and opacity (for individual citizens). Data protection legislation focuses on information (data) instead of knowledge (profiles, electronic footprints), PET's* focus on anonymisation / pseudonymity instead of counter-profiling which would allow some anticipation of the profiles that may be applied. To cope with RFID as an enabling technology for the age of 'everyware' the focus of both legal and technological tools needs to extend their protection of personal data to an effective access to knowledge. We need to complement PET's* with TET's* (transparency enhancing technologies).

8 Annex: Introduction to RFID Systems*

In this annex, technical details of RFID systems* are elaborated. Note that this is intended as an introduction to the various aspects of RFID systems*, the technical aspects of RFID will be further elaborated in the FIDIS Deliverable D3.7.

8.1 Basic operation of RFID systems*

Mark Gasson (Reading University)

The basic RFID system* consists of two main components, the small transponder*, more commonly known as a tag, which is attached to the item needing identification and the interrogator, or reader*, which in some cases is used to both power the tag and read its data without contact.

The tag is known as a *passive* transponder* if it is unable to function without the reader* since the reader* supplies the power to it. If the tag has its own power supply such as a battery, then it is an *active* transponder*. Note that 'reader*' is somewhat of a misnomer as the device in some cases can actually be used to write to the tag to change its data as well as reading from it. The basic components of the RFID system* are shown in Figure 8:

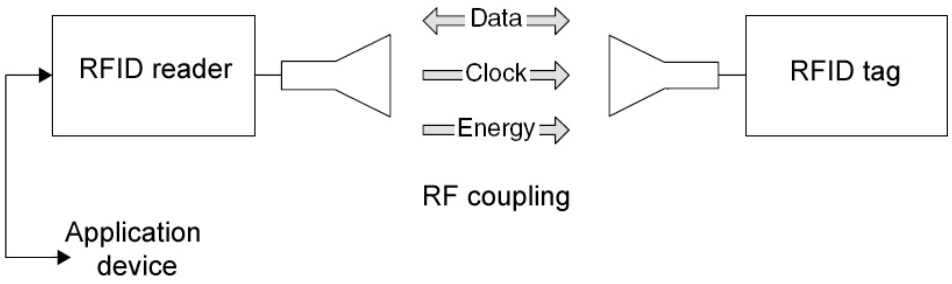

Figure 8: The two main components of the RFID system*

The range of RFID implementations available are broad, and are covered in more depth in other FIDIS deliverables. Here we will further elaborate on some of the key technical aspects of RFID systems*.

8.2 Types of RFID systems*

Since their conception, a plethora of RFID systems* have been developed. However, all of these systems are based on only a few basic operating procedures. The various operating methodologies can be derived from Figure 9.

Essentially, the RFID system* can operate based on one of two basic protocols: Full (or half) duplex (FDX / HDX) or sequentially (SEQ). During FDX / HDX the transponder* sends its data when the RFID reader* is asking for it (and in the passive case, supplying power to it). SEQ however requires the reader* to briefly turn off, during which time the tag sends it data.

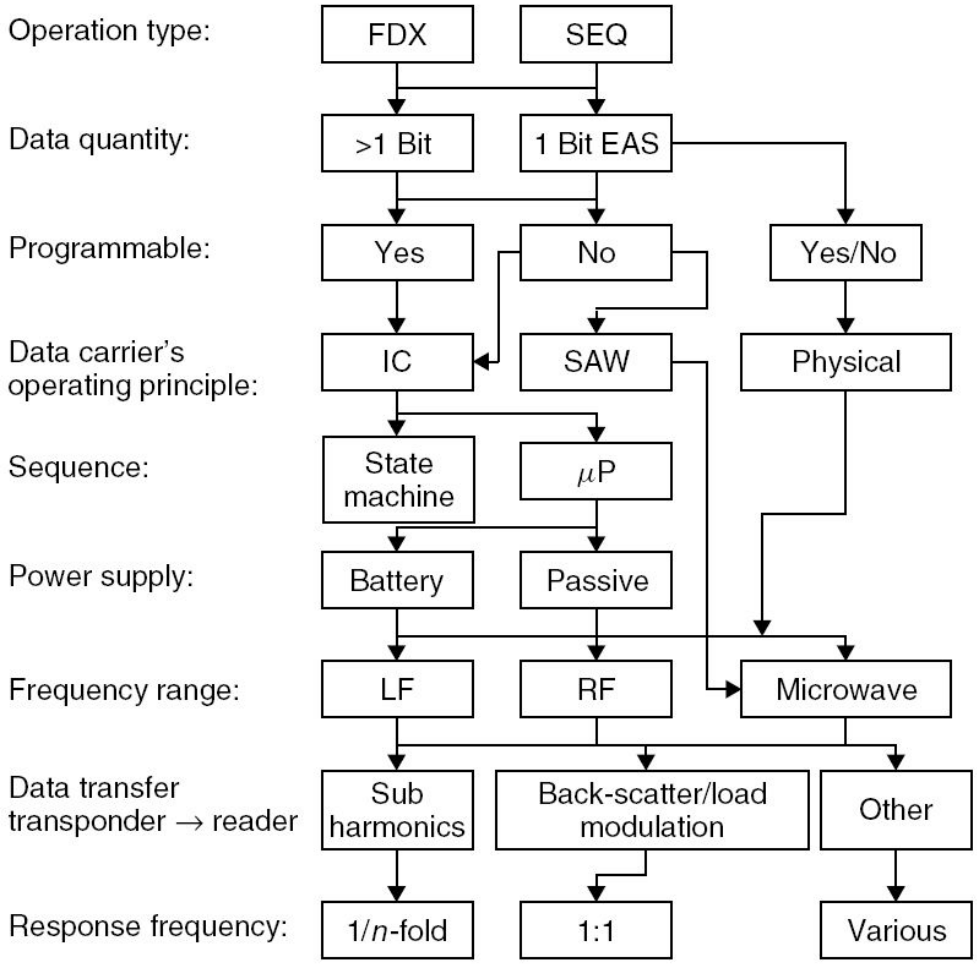

Figure 9: A flow diagram representing the various basic combinations of RFID systems* possible[106]

Typically, the data quantity a tag holds is in the region of a few bytes to a few kilobytes (sometimes referred to as n-bit). However, some tags only operate using 1 bit – that is the reader* can only tell if a tag is there or not, and nothing else. This is useful in applications such as shop security (Electronic Article Surveillance (EAS)) where you want an alarm to sound if a tag passes through the door *regardless* of what the tagged item is.

Some n-bit tags are programmable, that is the data that they contain can be changed by the 'reader'*. Systems that have this functionality typically use Induction Coupling (IC) as their

[106] (Integrated Silicon Design, 1996). The elements of this diagram will be elaborated in FIDIS deliverable 3.7.

means of communicating between reader* and tag, and most IC systems utilise passive tags. Simpler programmable tags contain simple logic (also known as a state machine) which can control read/write access or to perform fairly complex sequences as well as hold 'state variables'. More complex varieties use a microprocessor (uP) which allows some degree of complex operations to be performed, and is ultimately more flexible than the state machine solution.

8.3 Transmission Frequencies and Related Effects

RFID systems* can operate over a large range of frequencies depending on the mode of operation and the application, see Figure 10.

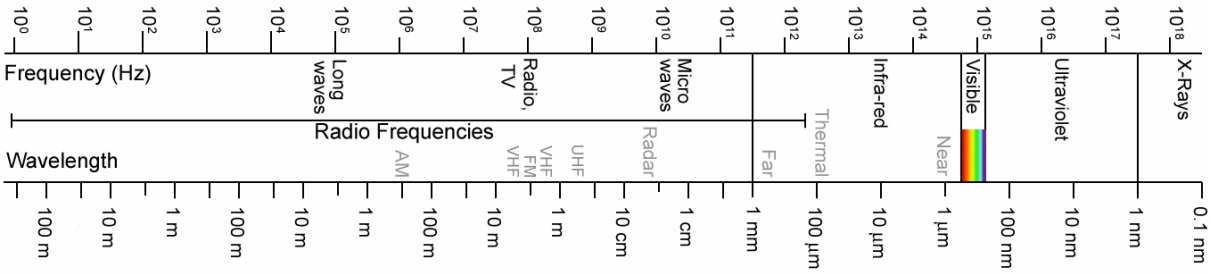

Figure 10: Illustration showing the broad range of frequencies within the electromagnetic spectrum that RFID systems* can utilise.

RFID transmission frequencies are roughly classified into the three ranges:

- LF (low frequency, 30-300 kHz),
- HF (high frequency)/RF radio frequency (3-30 MHz)
- UHF (ultra high frequency, 300 MHz-3 GHz)/microwave (>3 GHz).

RFID systems* that utilise frequencies between approximately 100 kHz and 30 MHz operate using inductive coupling, whereas microwave based systems in the frequency range 2.45–5.8 GHz are coupled using electromagnetic fields. However, the specific *absorption rate* (i.e. how much energy is lost as it passes through an object) of non-conductive substances (and water) is smaller by a factor of 100 000 at 100 kHz than it is at 1 GHz, so practically no energy is lost. The result of this is that systems operating at these frequencies will typically have a greater range. That said, lower frequency systems are noted for their improved object penetration over higher frequency ones. It should also be noted that the ranges achievable at higher frequencies are suitable for data transfer, but not for supplying power from the reader*, and as such these typically utilise active devices.

RFID systems* are also classified by range into:

- Close-coupling (0-1 cm),

- Remote-coupling (0-1 m),
- Long-range (>1 m) systems.

The achievable range is dependent not only on the frequency utilised, but also factors such as the positional accuracy of the transponder*, the minimum distance between several transponders* in practical operation and the speed of the transponder* in the interrogation zone of the reader* (Finkenzeller, 2003).

8.4 Selected Standards

Markus Hansen (ICPP)

With respect to RFID a number of standards are in place. They cover used frequencies, communication protocols between RFID tag* and reader* and formats for storing of data on RFID tags*. For the use of RFID in supply chains especially the following standards are important: ISO 14443 for the communication between RFID tag* and reader*, and the electronic product code* (EPC*), standardising how information with respect to products is coded on RFID tags*[107].

8.4.1 ISO 14443

ISO/IEC 14443 is an international norm for contactless identificaton smartcards with a communication range of up to 20 cm.

ISO/IEC 14443 has been established by Working Group 8 (WG8) of Subcommittee 17 (SC17) of the Joint Technical Comitee 1 (JTC1) of the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The standard series ISO/IEC 14443 consists of four parts and related amendments.[108] It is an international norm for contactless integrated circuit(s) cards with a communication range of 10 to 20 centimetres (proximity cards) used for identification purposes. A data transfer rate of up to 424 kBit/s can be established; the frequency used is 13,56 MHz. The four parts describe

- The physical characteristics (part 1),
- The radio frequency power and signal interface (part 2),
- The initialization and anticollision (part 3), and
- The transmission protocol (part 4).

ISO/IEC 14443 uses the terms PICC (proximity integrated circuit(s) card) for the contactless cards and PCD (proximity coupling device) for the readers*. It describes two types of cards,

[107] All web pages referred to in this chapter were accessed on 1st of August 2006.
[108] http://wg8.de/sd1.html

type A and type B. The main differences between these two types regard signal modulation methods,[109] coding schemes, and protocol initialization procedures.

ISO/IEC 14443 chips are used in a variety of products. E.g. one kind of Philips' MIFARE cards or Machine Readable Travel Documents (MRTD) according to ICAO document 9303[110] are based on ISO/IEC 14443.

While the norm defines communication ranges between 10 and 20 centimetres, experiments showed that the communication between tag and reader* can be eavesdropped at higher distances up to several metres (Finke, Kelter 2004). Such eavesdropping has already been used to show that the cryptographic key used to protect the communication between chip and reader* in case of Dutch MRTDs can be broken in approximately three hours.[111]

8.4.2 Electronic Product Code (EPC)*

EPC allows for unique identification and tracking of tagged objects via internet.*

EPCglobal Inc. is a non-profit organisation founded by GS1 (former EAN – European Article Numbering International) and UCC (Uniform Code Council), the two main barcode issueing associations.

EPC*, the Electronic Product Code* standardised by EPCglobal, is intended to replace EAN or UPC (Universal Product Code) numbers when RFID tags* replace barcodes as identifiers on products.

EPC* is a set of coding schemes for RFID tags*, originally developed by MIT AutoID Center. EPC* numbers start with a header identifying the encoding scheme used, which according to EPC Version 1.3[112] can be one of the following:

- General Identifier (GID), GID-96,
- Serialized version of the GS1 Global Trade Item Number (GTIN), SGTIN-96, SGTIN-198,
- GS1 Serial Shipping Container Code (SSCC), SSCC-96,
- GS1 Global Location Number (GLN), SGLN-96, SGLN-195,
- GS1 Global Returnable Asset Identifier (GRAI), GRAI-96, GRAI-170,
- GS1 Global Individual Asset Identifier (GIAI), GIAI-96, GIAI-202,
- DoD Construct, DoD-96.

The EPCglobal architecture allows the use of a variety of authentication technologies across its defined interfaces. It is expected, however, that the X.509 authentication framework will be widely employed within the EPCglobal network.[113]

---

[109] c.f. http://www.rfid-handbook.de/german/chipkarten.html#ISO14443
[110] c.f. http://www.icao.int/mrtd/Home/Index.cfm
[111] Harko Robroch, ePassport Privacy Attack, see http://www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf
[112] http://www.epcglobalinc.org/standards_technology/Ratified%20Spec%20March%208%202006.pdf
[113] http://www.epcglobalinc.org/standards_technology/ratifiedStandards.html

When an EPC* number is read, the reading device can identify the object via internet by accessing the Object Name Service[114] within the EPCglobal network.[115] The EPCglobal Networks aims at exchanging data in real time to allow tracking of products. An EPC* number contains:

- Header, which identifies the length, type, structure, version and generation of EPC*,
- Manager Number, which identifies the company or company entity ,
- Object Class, similar to a stock keeping unit,
- Serial Number, which is the specific instance of the Object Class being tagged.

Additional fields may also be used as part of the EPC* in order to properly encode and decode information from different numbering systems into their native (human-readable) forms.[116]

EPC* uses Object Name Service (technically based on DNS) to allow for unique identification of tagged objects (as opposed to identification of object class with barcodes).

[114]http://www.epcglobalinc.org/standards_technology/EPCglobal_Object_Naming_Service_ONS_v112-2005.pdf
[115]http://www.epcglobalinc.org/about/EPCglobal_Network.pdf
[116]http://www.epcglobalus.org/Network/Electronic%20Product%20Code.html

9 References

Legal texts

Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data, Council of Europe, European Treaty Series No. 108, Strasbourg, 28/01/1981.

Convention on Cybercrime, Budapest, 23.XI.2001. Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Convention of Rome on the Law applicable to contractual obligations opened for signature in Rome on 19 June 1980 (80/934/EEC), *Official Journal L 266, 09/10/1980 p. 0001 - 0019*

Council Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999, *Official Journal* L 141 , 04/06/1999, p. 0020 – 0021.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *Official Journal* L69/67, 16.3.2005.

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *Official Journal L 012* , 16/01/2001 p. 0001 – 0023.

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *Official Journal L* 210 , 07/08/1985 p. 0029 – 0033.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. *Official Journal* L 095, 21/04/1993 P. 0029 – 0034.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') *Official Journal* L 178, 17/07/2000 P. 0001 – 0016.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *Official Journal* L 13, 19/01/2000. P. 0012 -0020.

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, Official Journal, L 281/31 – L 281/39.

Directive 2006/24/Ec of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal* L105/54, 13.4.2006.

Bibliographical References

ACM Newstrack, 'Embedded Risks', *Communications of the ACM*, Assn. For Computing Machinery, New York, 2006, http://www.acm.org/pubs/cacm/newstrack/2006/embeddedrisks.html

Alheit, K., 'The applicability of the EU Product Liability Directive to Software', *The Comparative and International Law Journal of South Africa*, Vol. 3, No. 2 , University of South Africa, Institute of Foreign and Comparative Law, Pretoria, 2001, pp. 188 - 209.

Art. 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, WP105, 19 January 2005, Available at;
http://www.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Art 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace*, WP 55, 29 May 2002.

Art 29. Data Protection Working Party, *Opinion 8/2001*, WP 48, 13 September 2001.

Averill, J.R, 'Personal control over aversive stimuli and its relationship to Stress', *Psychological Bulletin*, Vol. 80, Apa Journals, Washington, 1973, pp. 286-303.

Audio-ID Center, 'Technology Guide', 2003, pp 24. Download via http://interval.hu-berlin.de/downloads/rfid/technologische%20grundlagen/Technology_Guide.pdf

Backhouse, J., (Ed.). 'Structured Account of Approaches on Interoperability', *FIDIS Work package 4, Deliverable D4*.2, 2005.

Bandura, A., 'Human agency in social cognitive theory', *American Psychologist*, Vol. 44, No. 9, Apa Journals, Washington, 1989, pp. 1175-1184.

Bijker, W.E, Hughes, T.P., Pinch, T. (Eds), *The social construction of technological systems, New Directions in the Sociology and History of Technology*, MA, MIT Press, Cambridge, 1987.

Bijker, W.E., 'The Social Construction of Fluorescent Lighting, Or how an Artifact Was Invented in its Diffusion Stage', in Bijker W.E. and Law J. (Eds.) *Shaping Technology/building society. Studies in sociotechnical change*, MIT Press, Cambridge, 1997, pp. 75 – 104.

Bimber, B., 'Three Faces Of Technological Determinism', in Smith, M. R,. , Marx, L., (Eds.), *Does Technology Drive History? The Dilemma of Technological Determinism*, MIT Press, Cambridge, 1994, pp. 79 – 100.

Bohn, L. et al., 'Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing', Institute for Pervasive Computing, ETH Zurich, Switzerland, 2004, p. 24. Available at: http://www.vs.inf.ethz.ch/publ/papers/socialambient.pdf

Boone, T., 'Can Bar Codes and RFID Co-Exist?', *Inbound Logistics, IT Matters*, December 2005. Available at: http://www.inboundlogistics.com/articles/itmatters/itmatters1205.shtml

Borking, J., 'Der Identity Protector', *Datenschutz und Datensicherheit*, Vieweg Verlag, Wiesbaden, 11/1996, pp. 654-658.

Borking, J., Raab, C. D., 'Laws, PETs and Other Technologies for Privacy Protection', *The Journal of Information, Law and Technology*, Vol. 1, Universities of Warwick and Strathclyde, United Kingdom, , 2001. Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/

Busch, D., 'Indirect Representation and the Lando Principles. An Analysis of Some Problem Areas from the Perspective of English Law', *Electronic Journal of Comparative Law*, Vol. 2, No. 3, December 1998.

Brutsaert, H., *Sociologie*., Derde Editie, Vakgroep Sociologie Universiteit Gent, 1995.

Callon, M., 'Techno-economic network and irreversibility', in Law J. (eds.), *A sociology of monsters. Essays on power, technology and domination*, Routledge, London, 1991, pp. 132-164.

Capgemini, 'RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business', *Report of Capgemini*, 2005. Available at: http://www.nl.capgemini.com/resources/thought_leadership/rfid_and_consumers_what_european_consumers_think_about_radio_frequency_identification_and_the_implications_for_busines/

Davis, F. D., 'Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology', *MIS Quarterly*, Vol. 13, No. 3, Management Information Systems Research Center, Minnesota, 1989, pp. 319-340.

Delaney, H., Van de Zande, R., (eds.), *A Guide to the EU Directive Concerning Liability for Defective Products (Product Liability Directive)*, 2001, pp 1. Available at: http://ts.nist.gov/ts/htdocs/210/gsig/eu-guides/gcr-824/product-liability-guide-824.pdf

Department of Commerce Washington D.C., 'Radio Frequency Identification. Opportunities and challenges in Implementation', Department of Commerce, Washington DC, April 2005.

Desai, M.S., Oghen, J., Richards, T.C., 'Information Technology Litigation and Software Failure', *The Journal of Information, Law & Technology*, Vol. 2, Universities of Warwick and Strathclyde, United Kingdom, 2002. Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/desai/.

Die Zeit, 'Soll das Auto die Werkstatt alarmieren?', Nr.45, ZEIT Online-GmbH (Die Zeit),Oxford, 03.11.2005. Available at: http://www.zeit.de/2005/45/Interv_Spiekermann (accessed on 16th of May 2006).

Eckfeldt, B., 'What Does RFID Do for the Consumer', *Communications of the ACM*, Vol. 48, No. 9, Assn. For Computing Machinery, New York, 2005, pp. 77-79.

eGov monitor, 'Q&A: Viviane Reding, EU Commissioner for Information Society and Media', Published on 27 March 2006, Knowledge Asset Management Limited, London, 2006. Available at: http://www.egovmonitor.com/node/5302 (accessed on 3 April 2006).

European Data Protection Supervisor (EDPS), 'Annual Report 2004', available online at http://www.edps.eu.int/publications/annual_report/2004/Annual_Report_2004_EN.pdf (accessed 18 Mai 2006)

European Data Protection Supervisor (EDPS), 'Annual Report 2005'., Available at: http://www.edps.eu.int/publications/annual_report/2005/AR_2005_EN.pdf (accessed 18 Mai 2006)

European Group on Ethics of Science and New Technologies, 'Ethical aspects of the ICT implants in the human body', *Opinion*, No. *20*, March 2005. Available at: http://147.67.4.5/comm/european_group_ethics/docs/avis20compl.pdf

European Group on Tort Law. 'Principles of European Tort Law, Text and Commentary.',SpringerWienNewYork, 2005. Available at: http://www.egtl.org/.

Finke, T., Kelter, H., *Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*, Bonn, 2004. Available at: http://www.bsi.bund.de/fachthem/rfid/Abh_RFID.pdf

Finkenzeller, K., *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition*, Wiley & Sons, Australia, 2003.

Fishkin, K. P., Sumit, R., 'Enhancing RFID Privacy via Antenna Energy Analysis', *MIT RFID Privacy Workshop*, MIT Media Lab, Cambridge, November 2003. Also Intel Research Seattle Technical Memo IRS-TR-03-012, November 2003.

Fleck, M. et al., 'From Informing to Remembering: Ubiquitous Systems in Interactive Museums', *IEEE Pervasive Computing*, Vol.1, No. 2, IEEE Computer Society, April 2002, pp. 13-21.

Floerkemeier, C., Schneider, R., Langheinrich, M., 'Scanning with a purpose – Supporting the Fair Information Principles in RFID-Protocols', Zurich, 2004. Available at: http://interval.hu-berlin.de/downloads/rfid/prevention/floerkem_scanning%20with%20a%20purpose.pdf

Friedewal, M., Da Costa, O. (Eds.), 'Science and Technology Roadmapping: Ambient Intelligence in Everyday Life (AmI@Life)', *final report of the JRC-IPTS/ESTO project "Ambient Intelligence in Everyday Life Roadmap,"*, Seville, 2003. Available at: http://fiste.jrc.es/download/AmIReportFinal.pdf

Friedewald, M., Lindner, R., Wright D. (eds.), 'Threats, Vulnerabilities and Safeguards in Ambient Intelligence', *SWAMI project Deliverable D3,* 2006. Available at http://swami.jrc.es

Garfinkel, S.L., Juels, A., Pappu, R., 'RFID privacy: an overview of problems and proposed solutions', IEEE *Security and Privacy,* Vol. 3, No. 3, IEEE Computer Society Press, May-June 2005, pp. 34-43.

Garfinkel, S.L., Rosenberg B. (eds). *RFID: Applications, Security, and Privacy*, Addison-Wesley Professional, Boston, 2005.

Garreau, J., *Radical Evolution. The Promise and Peril of Enhancing Our Minds, Our Bodies – and What It Means to Be Human*, Double Day, New York 2005.

Gasson, M., Meints, M., Warwick, K. (eds.), *FIDIS Deliverable D3.2 – A Study on PKI and Biometrics*, 2005. Available at: http://www.fidis.net/487.0.html#c818

Greenfield, A., *Everyware. The dawning age of ubiquitous computing*, New Riders, Berkeley 2006.

Gossett, S., 'Paying for Drinks with Wave of the Hand - Clubs Goers in Spain Get Implanted chips for ID Payment Purposes', World Net Daily 2004. Available at: http://worldnetdaily.com/news/article.asp?ARTICLE_ID=38038

Gripenberg, P., 'ICT and the shaping of Society. Exploring Human – ICT relationships in everyday life', *Publications of the Swedish School of Economics and Business Administration*, nr. 143, 2005. Available at http://www.hanken.fi/portals/pubmanager/pdf/143-951-555-874-3.pdf

Günther, O., Spiekermann, S., 'RFID and the perception of control: the consumer's view', *Communications of the ACM*, Vol. 48, No. 9, Assn. For Computing Machinery, New York, September 2005, pp. 73 - 76. Available at: http://portal.acm.org/citation.cfm?id=1082023&coll=ACM&dl=ACM&CFID=75922713&CFTOKEN=76060018

Hanseth, O., Monteiro, E., 'Socio-technical webs and actor network theory', chapter 6 of *Understanding Information Infrastructure*, 1998. Available at: http://heim.ifi.uio.no/~oleha/Publications/bok.6.html#pgfId=913144 (accessed on 3 April 2006).

Hilty, L. et al., 'The Precautionary Principle in the Information Society, Effects of Pervasive Computing on Health and Environment', *Report of the Centre for Technology Assessment*, February 2005.

Howcroft, D., Mitev, N., Wilson, N., 'What we may learn for the social shaping of technology approach', in Mingers, J., Willcocks, L. (eds.) *Social theory and philosophy for information systems*; Wiley and Sons ltd., Australia, 2004, pp. 329 – 371.

Hsi, S., Fait, H., 'RFID enhances visitors' museum experience at the Exploratorium', *Communications of the ACM*, Vol. 48, No. 9, Assn. For Computing Machinery, New York, September 2005, pp 60 -65.

Ingdahl, W., 'RFID in the euro notes?', *The Sprout*, May 2004. Available at: http://www.eudoxa.se/content/archives/2004/06/rfid_in_the_eur.html.

Integrated Silicon Design Pty Ltd., 'Training Manual', Adelaide, Australia, 1996.

Italian DPA (Garante per la protezione dei dati personali), 'Loyalty cards and safeguards for the consumers: guidelines applying to loyalty programmes', Web No. 1109624, dated 24 February 2005. Available at: http://www.garanteprivacy.it/garante/doc.jsp?ID=1109624

ITU, 'The Internet of things', *ITU Internet Reports 2005*, 7th edition. Available at : www.itu.int/internetofthings

Jay, R., Hamilton, A., *Data Protection- law and Practice,* Sweet & Maxwell, London, 2003, chapter 3 -39.

Juels, A. and Brainard, J.,'Soft Blocking: Flexible Blocker Tags on the Cheap', in De Capitani di Vimercati, S., Syverson P., (eds), *Workshop on Privacy in the Electronic Society (WPES)*, 2004.

Juels, A., Rivest, R. L., Szydlo, M., 'The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy', *8th ACM Conference on Computer and Communications Security*, ACM Press, Washington, 2003, pp 103- 111.

Knospe, H., Pohl, H., 'RFID Security', *Information Security Technical Report*, Vol. 9, No. 4, Elsevier Ltd., Oxford, 2004, p 30 – 41. Available at: http://www.securitywireless.info/upload/dl/Rfid/RFID_Security_ISTR.pdf

Kafka, F., *The Trial*, translation by Breon Mitchell, Schocken, New York, 1999

Latour, B., *Reassembling the Social- An Introduction to Actor-Network-Theory*, Clarendon Lectures in Management Studies, Oxford University Press, USA, 2005.

Law, J., Hassard, J., (Eds), *Actor Network Theory and after*, Blackwell Publishers/The Sociological Review, Oxford, UK, 1999.

Lee, H., et al., 'Privacy threats and issues in mobile RFID', *ARES conference*, Vienna, April 2006.

Legal IST, 'Legal issues of RFID technology', 2006, p 30. Available at: http://www.rfidconsultation.eu/docs/ficheiros/Legal_issues_of_RFID_technology_LEGAL_IST.pdf

Liebenau, J. and Backhouse J., *Understanding Information: An Introduction*, Macmillan Press, Basingstoke and London, 1990.

Locquenghien von, K., 'On the Potential Social Impact of RFID-Containing Every-day Objects', *Science, Technology and Innovation Studies,* Vol.2, University of Dortmund , Germany, 2006, pp. 57-78.

Lyon, D., 'Identity Card: social sorting by database', *Internet Issue Brief No. 3,* Oxford Internet Institute, November 2004.

MacKenzie, D., Wajcman, J., *The social shaping of technology: how the refrigerator got its hum* . Open University Press, Philadelphia, 1985.

Magnus, U., Micklitz, H.W., Institut Für Europaïsches Wirtschafts- Und Verbraucherrecht E.V. From Berlin (View), 'Comparative Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services', *A study commissioned by the European Commission, Final Report,* April 2004. Part A: General Part. Part B: Survey over the Contract and Tort Liability in the Reported Legal Systems. Part C: The Specific Part – Medical Services, Leisure, Tourism and Public Utilities. Part C is available at: http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportabc_en.pdf Part D is available at: http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf

Meints, M., Hansen, M. (Eds.), 'Study on ID Documents', *FIDIS Work package 3, Deliverable D3.6,* Frankfurt a.M., 2006. Available at: http://www.fidis.net/487.0.html

Meints, M., 'Protokollierung bei Identitätsmanagementsystemen', *Datenschutz und Datensicherheit,* Vieweg Verlag, Wiesbaden, 5/ 2006, pp. 304-307,.

Metro Group Future Store Initiative, 'The Future begins now. Technologien', January 17th 2006. Available at: http://www.future-store.org/servlet/PB/-s/68lq0912kjivf4hqf0149asnp3spni0/menu/1007338_l1_yno/index.html

Miedema, F., Post, B., *Evaluatie pilot elektronische volgsystemen,* IST, Nijmegen, January 2006.

Molnar D., Stapleton-Gray, R., Wagner, D., 'Killing, Recoding and Beyond', Chapter 23 of Garfinkel S., Rosenberg, B., *RFID Applications, Security and Privacy,* Addison Wesley Professional, Boston, 2005.

Molnar, D., Soppera, A., Wagner, D., 'Privacy for RFID Through Trusted Computing' *Workshop on Privacy in the Electronic Society – WPES,* Alexandria, Virginia, USA, ACM Press, November 2005.

Monteiro E. 'Actor Network theory and information infrastructure', in Ciborra, C.U., (Ed.), *From Control to Drift,* Oxford University Press, Oxford, 2000, pp. 71-86, Available at : www.idi.ntnu.no/~ericm/ant.FINAL.htm (accessed on 10th of March 2006).

Mullen D., Moore, B., 'Automatic Identification and Data Collection: What the future Holds', Chapter 1 of Garfinkel, S., Rosenberg B., (Eds.), *RFID Applications, Security and Privacy*, Addison-Wesley Professional, Boston, 2005, pp. 608.

Natarajan V., Balasubramanian A., Mishra S., Sridhar R., 'Security for Energy Constrained RFID System', *Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies* (*AutoID'05*), 2005.

National Academy of Engineering, 'Technically speaking, What has been done? The international experience', *The National Academy of Sciences*, USA, 2006. Available at: http://www.nae.edu/nae/techlithome.nsf/weblinks/KGRG-55X5R7?OpenDocument

Neumann, P.G., Weinstein, L., 'Inside Risks: Risks of RFID', *Communications of the ACM*, Vol. 49, No. 5, Assn. For Computing Machinery, New York, May 2006, pp. 136.

Pinch, T., Bijker, W.E.,'The social construction of facts and artifacts: or how the sociology of science and technology might benefit each other', in Bijker, W;E., Hughes, T.P., Pinch, T., (eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology;* MA MIT Press, Cambridge, 1987, pp. 399-441.

Punie Y., 'A social and technological view of Ambient Intelligence in Everyday Life: What bends the trend?' *The European Media and Technology in Everyday Life Network*, EMTEL2; Key Deliverable Work Package 2 September 2003EC DG JRC IPTS, Sevilla (EUR 20975), 2003.

Punie, Y., et al., 'Dark scenarios on ambient intelligence – Highlighting risks and vulnerabilities', *SWAMI project, deliverable 2*, January 2006. Available at: http://swami.jrc.es/pages/documents/SWAMI_D2_scenarios_Final_ESvf_002.pdf

Reed, Ch. and Welterveden A., 'Liability', in Reed, Ch., and Angel, J. (Eds.): *Computer Law*, Fourth Edition, Blackstone, London, 2000, pp. 101 - 130.

RFID Journal, 'General RFID Information, FAQ Will RFID replace bar codes?' Available at http://www.rfidjournal.com/faq/16/51

RFID Journal, 'RFID for Your Shopping Cart', July 2003. Available at: http://www.rfidjournal.com/article/articleview/489/1/1/

Rieback, M. R. Crispo, B., Tanenbaum, A. S., 'RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management.' *Proc. 10th Australasian Conference on Information Security and Privacy. (ACISP 2005)*, Brisbane, Australia, July 2005. Available at http://www.cs.vu.nl/~melanie/rfid_guardian/papers/acisp.05.pdf

Rieback, M.R., et al., 'Is your Cat infected with a Computer Virus*?', Fourth Annual IEEE International Conference on Pervasive Computing and Communications, 2006. PerCom 2006*, Los Alamitos, IEEE Computer Society, 2006. pp. 169-179. Available at: http://www.rfidvirus.org/index.html

Rieback, M.R, et al., 'Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags', *Proceedings of SPW 2005*, Cambridge, 2005. Available at: http://www.rfidguardian.org/papers/sec_prot.05.pdf

Rip, A., 'Science and Technology Studies and Constructive Technology Assessment', *EASST Review*, European Association for the Study of Science and Technology, Surrey, September 1994. Available at: http://www.easst.net/review/sept1994/rip (accessed on 8th of June 2006) .

Robey, D., 'The paradoxes of transformation', in Sauer, C., Yetton, P.W. (eds.), *Steps to the Future: Fresh thinking on the management of IT based organizational transformation*, Jossey Bass Publications, San Fransisco, 1997, pp. 209-229.

Rötzer, F., 'Der erste RFID-Virus wurde präsentiert', *Telepolis*, March 15, 2006. Available at: http://www.heise.de/tp/r4/artikel/22/22252/1.html

Royer, D. (ed.), Deliverable D11.1: Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity, Work Package 11, 2006. Available at: www.fidis.net/fidis_del.0.html.

Schermer, B., 'Criminaliteit en RFID', in Zwenne, G.J., Schermer, B., (eds.), *Privacy en andere juridische aspecten van RFID*, Elsevier Juridisch, 's-Gravenhage, 2005, pp. 83-96.

Schreurs, W., Hildebrandt, M., Gasson, M., Warwick, K., 'Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence', *FIDIS Work Package 7, Deliverable D7.3*, 2005, p 68. Available at: www.fidis.net

Singsangob, A., *Computer Software and Information Licensing in Emerging Markets, The Need for Viable Legal Framework*, Kluwer Law International, Alphen a/d rijn and London, 2003.

Smith, M. R., Marx, L., (Eds.), *Does Technology Drive History? The Dilemma of Technological Determinism*, MIT Press, Cambridge, 1994.

Solove, D., *The Digital Person: Technology And Privacy In The Information Age*, New York University Press, New York, 2004.

Spiekermann, S., 'Perceived Control: Scales for Privacy in Ubiquitous Computing Environments', *10th International Conference on User Modelling*, Edinburgh, Scotland, July 2005. Available at: http://interval.hu-berlin.de/downloads/rfid/neuste%20forschungsergebnisse/UM05_Spiekermann.pdf

Spiekermann, S., Rothensee, M., ,'Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing', Humboldt-Universität, Berlin, July 2005. Available at: http://interval.hu-berlin.de/downloads/rfid/neuste%20forschungsergebnisse/SocioPsychofak.pdf

Spychips.Com, 'Future Store Overview', *Background Metro "Future Store" Special Report.* Available at: http://www.spychips.com/metro/overview.html

Spychips.Com, 'Scandal: The RFID Tag Hidden in METRO's Loyalty Card', *The METRO "Future Store", Special Report.* Available at: http://www.spychips.com/metro/scandal-payback.html

Stamper, R., et al., 'Understanding the roles of signs and norms in organizations-a semiotic approach to information systems design', *Behavior and Information Technology*, Vol. 19, No. 1, Taylor and Francis, Abingdon, 2000, pp 15-28.

STREP, 'NO-REST, Networked Organisations – Research into Standards and Standardisation', *IST, D07–Report on 'The Dynamics of Standards I: Research Findings'*, 2005.

Sunstein, C., *Republic.com*, Princeton University Press, Princeton and Oxford, 2001.

Sunstein, C., *Laws of Fear: Beyond the Precautionary Principle*, Cambridge University Press, Cambrigde, 2005.

Tien, L., 'Doors, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment Law', *DePaul Law Review, Vol. 54*, DePaul University College of Law, Chicago, 2005, pp. 873-908.

Van Eecke, P., Skouma, G., 'RFID and Privacy: A difficult Marriage?', in Paulus, S., Pohlmann, N., Reimer , H., (eds.), *ISSE 2005 Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 2005 Conference*, Vieweg ISSE, 2005, pp. 169-178.

Von Bar C., Lando, O., Swann, S., 'Communication on European Contract Law: Joint Response of the Commission on European Contract Law and the Study Group on a European Civil Code', *European Review of Private Law*, Vol. 10, No. 2, Wolters Kluwer, Alphen a/d rijn and London, 2002, pp. 183 – 248.

Verbeek, P-P., *What Things do. Philosophical Reflections on Technology, Agency, and Design*, The Pennsylvania State University Press, Pennsylvania, 2005

Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V, 'Der Metro-Skandal'. Available at: http://www.foebud.org/rfid/metro/

Weiser, M., 'Some Computer Science Issues in Ubiquitous Computing', *CACM*, Vol. 36, No. 7, Assn. For Computing Machinery, New York, July 1993, pp. 74- 84, available at: www.ubiq.com/hypertext/weiser/UbiCACM.html,

Williams, R., Edge, D., 'The social shaping of technology', *Research Policy*, Vol. 25, No. 6, Elsevier, Amsterdam and London, 1996, pp. 856 – 899.

10 Abbreviations & Glossary

AI* – artificial intelligence

DRM* – digital rights management

EPC*- electronic product code

HCI* – human computer interaction

MITM* – man-in-the-middle attack

MRTD – machine readable travel documents

PET* – privacy enhancing technology

RFID – radio frequency identification

SCM – supply chain management

TET* – transparency enhancing technology

actuator - the mechanism by which an agent acts upon an environment. The agent can be either an artificial intelligent agent or any other autonomous being (human, other animal, etc). (wikpedia April 2006)

artificial intelligence (AI) - intelligence exhibited by an artificial entity. Such a system is generally assumed to be a computer; also a branch of computer science; also a scientific discipline, focused on providing solutions to real life problems (in medicine, engineering, the military). (wikipedia April 2006)

digital rights management (DRM) - umbrella term referring to any of several technologies used to enforce pre-defined policies controlling access to software, music, movies, or other digital data and hardware. In more technical terms, DRM* handles the description, layering, analysis, valuation, trading and monitoring of the rights held over a digital work. In the widest possible sense, the term refers to any such management. [wikipedia April 2006]

distributive group profile – a group profile with distributive properties, which means that the 'properties are valid for each individual member of the group' (Custers 2005:61), this is for instance the case for the group of members of the group of bachelors, who share the property of not being married. Most group profiles generated in the process of data mining are non-distributive.

electronic product code (EPC) - a code electronically recorded on an RFID tag* [wikipedia April 2006]

human computer interaction (HCI) - the refers to how people (*the users*) interact with a particular machine, device, computer program or other complex tool (*the system*). An important aspect of HCI research is the development and optimisation of user interfaces.

man-in-the-middle attack (MITM) – (in cryptology) an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised

non-distributive group profile - a group profile with non-distributive properties, which means that the 'property is valid for the group and for individuals as members of the group, though not for those individuals as such' (Custers 2005:61), this is for instance the case for members of the group of smokers, who have a specific chance to develop long cancer, but depending on their age, gender and life-style this chance may vary.

personalised profiles – a personalised profile is a profile that is highly specific to a particular person, either based on data collected from this person and/or based on group profiles that may have been combined for a specific context to allow customised servicing of an individual customer or very specific knowledge about a person with regard to potential criminal or security risks. See FIDIS deliverable 7.2, section 3.3.

PETs – are 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 data; all without losing the functionality of the data system." (Borking 1996, translation taken from Borking, Raab 2001).

RFID system - may consist of several components: tags, tag readers*, edge servers, middleware, and application software. The purpose of an RFID system is to enable data to be transmitted by a mobile device, called a tag, which is read by an RFID reader* and processed according to the needs of a particular application. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc. [wikipedia April 2006]

RFID tag - a small object that can be attached to or incorporated into a product, animal, or person. RFID tags contain silicon chips and antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver* [wikipedia April 2006]

reader – see transceiver*

sensor - a physical device or biological organ that detects, or *senses*, a signal or physical condition and chemical compounds; an electronic sensor is a type of transducer* [wikipedia April 2006]

TETs* – transparency enhancing technologies, which have not been developed yet. Their function is not the history management of the data of a data subject, but the anticipation of profiles that may be applied to this a particular data subject. This concerns personalised profiles* as well as distributive* or non-distributive group profiles*, possibly constructed out of anonymous data. The point would be to have some idea of the selection mechanisms (application of profiles) that may be applied, allowing a person adequate anticipation. To be able to achieve this the data subject needs access - in addition to his own personal data and a profiling / reporting tool - to additional external data sources, allowing some insight in the activities of the data controller. Based on this additional information the data subject could perform a kind of counterprofiling. TETs* will be further discussed in deliverable 7.9.

transceiver - a device that has a transmitter and a receiver which are combined [wikipedia April 2006]

transducer - a device, usually electrical or electronic, that converts one type of energy to another for the purpose of measurement or information transfer. Most transducers are either sensors* or actuators [wikipedia April 2006]

transponder - a receiver-transmitter* that will generate a reply signal upon proper electronic interrogation. [wikipedia April 2006]

ubiquitous computing - the method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user [Mark Weiser 1993, available at: www.ubiq.com/hypertext/weiser/UbiCACM.html]