FIDIS

Future of Identity in the Information Society

Title:	"D 7.6 Workshop on AmI, Profiling and RFID"
Author:	WP7
Editors:	Els Soenens, Mireille Hildebrandt (VUB)
Reviewers:	Denis Royer (JWG, Germany)
Identifier:	D7.6 Workshop
Type:	[Template]
Version:	0.10
Date:	Wednesday, 15 February 2006
Status:	[Template]
Class:	[Public]
File:	D7.6 Report

Summary

The second workshop of the WP 7 titled 'AmI, RFID and Profiling' (D7.6) was organized at the Vrije Universiteit Brussel on January 20th as preparation for deliverable 7.7. This report records the participants to the workshop and their presentations and includes the relevant issues and the proposed structure of the report on 'AmI, RFID and Profiling', discussed during the meeting. On top of that it summarises the decisions taken during the workshop on the contributions to and content of the report.

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	25.01.2006	• First version (Els Soenens)
0.2	31.01.2006	• Chapter on Decisions taken at the Workshop (Mireille Hildebrandt)
0.3	31.01.2006	• Internal review (Martin Meints)

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)*
1,3,4,5,6	Els Soenens
2 (Decisions made during the workshop)	Mireille Hildebrandt, Martin Meints
…	…

Table of Contents

1 Executive Summary

This is the report of the workshop on AmI, RFID and profiling, helt at the Vrije Universiteit Brussel at 20.01.2006. This second workshop of WP 7 was organized as a kick off meeting to prepare for the report D7.7 on RFID, AmI and Profiling, to be submitted by the end of July 2006.

Note: This section is mandatory for all deliverable and should help to get an overview of the topics covered in the document.

2 Decisions made during the workshop

In the following sections the presentations of the various participants are made available, starting with a summary of the issues that were highlighted by participants in their abstracts as relevant for D7.7. It also includes a draft for the contents and structure of the report.

In this section the decisions made regarding the contributions to the report by various partners are summarised, including the major issues to be dealt with per chapter.

2.1 Editors, internal reviewers and time table

The editors of the report will be Martin Meints (ICPP) and Mireille Hildebrandt (VUB). Claudia Diaz and Denis Royer will take care of the internal FIDIS review.

The following time table was agreed:

- 15 March abstract
- 15 April 1st version contributors
- 1 May comments editors
- 15 May final version contributors
- 1 June final version report; internal review
- 15 June comments internal reviewers
- 1 July off to the Commission

2.2 The structure of the report

Below we summarise the general outline for the report, including a set of issues identified as relevant within one or more chapters, by FIDIS partners. It will evidently not be possible to deal extensively with all the issues, but they should serve as indications of the focus of the relevant chapters. At the same time the enumeration of relevant issues is by no means exhaustive. It seems obvious that many of the social aspects are directly or indirectly related to the technological and legal aspects, demanding cross-border references between the chapters.

2.2.1 Chapter 1: Profiling AmI and RFID

In this chapter the emphasis will be on the link between RFID, profiling and AmI. We will introduce the way in which RFID may develop into one of the preconditions for AmI, due to the production of data that will allow profiling. After elaborating a shared working definition for RFID, the emphasis will be placed on the RFID-*system* that allows the collection and processing of RFID-related data. It will be made clear how both the RFID-system, mobile

communication and readers that trace RFID tags and linked subjects in their environment, will enable the kind of tracking for the offline world that we are already familiar with when online.

The chapter will include 2 or 3 examples of existing, planned or tested solutions to elaborate the links between these topics and key issues of RFID as such. ICPP will elaborate the example of the Metro future store, KU will elaborate an example of supply chain tracking and GUF will provide an example relating to LBS . On top of that IPTS will develop two future scenarios with possible relevance for the legal chapter (especially liability issues). The examples and scenario's are meant to illustrate the links between RFID, profling and AmI and should include a first impression of the social implications (risks and benefits) of RFID technologies.

Relevant issues at this point are:

- explain what kind of identification is possible and *necessary* within an RFID-tagged AmI environment?
- explain how checking and matching with centrally stored data implies the creation of a database infrastructure, which will enable massive profiling;
- explain how AmI both presumes and produces an extensive profiling infrastructure;
- explain how LBS (that can be seen as a forerunner of AmI) can be based on RFID location data;
- explain the risks of illegal data transfer and data laundering, due to the lack of effective transparency;
- could it be that targeted servicing, LBS and AmI will raise the level of spam without delivering promised benefits that outweigh the disadvantages of ever increased spamming?
- acceptance of AmI and RFID will depend on trust and usability. Consumers don't seem to 'buy' the 'consumer focus narrative'; will the required paradigm shift towards AmI enabling technologies (RFID and other mobile identifications) occur and what could facilitate such a shift; should we appreciate the attempt to introduce RFID at gadget level facilitating wider dissemination and function creep instead of a well-informed consensus on extended use of RFID?

2.2.2 Chapter 2: Technological issues

This chapter will refer to the work done in deliverable 3.7 and restrict its scope to basic aspects of RFID-implementation, following the TOC for 3.7, to provide an overview on the possibilities and limitations (including essential security problems) of this technology. The focus should be kept on AmI-related applications. As far as the reference to 3.7 is concerned ICPP will contribute, with added input from Mark Gasson of Reading University.

Relevant issues at this point are:

- could it be that the introduction of microcontrollers will reduce (or take away) the need to create a back-end system?
- RFID enables (among others) passive authentication (in this case by unrecognised, indirect identification of a linked data subject). Is it possible to develop AmI environments that preclude unauthorised access to RFID-devices?
- biometrics, RFID and LBS are different, but potentially converging forerunners of AmI. Biometrics and RFID are more on the side of passive authentication driven scenarios, traditional LBSes are potentially more on the track of using identity managers for AmI-services. The borderline between passive and active authentication is important, as today we don't know any technical safeguards against passive authentication as far as we don't try to implement something like data management (which sensor, when and where received this data?) for any sensor data (DRM-like approach) on earth.
- will AmI function with pseudonyms?RFID seems to focus on the tracking of things. How could this imply or facilitate the tracking of persons?
- in which ways are supplementation and/or modification and of tag data possible by the data reader?
- do RFID-technologies enable the realisation of the data minimisation principle, the finality principle and the principle of accuracy of data (reference to the legal chapter)?
- who is data controller in the smart home? If the rfid *system* includes online connections with service providers, are they data controllers and/or is the software provider data controller? To what extent can the user control the data?
- explain briefly that since profiling enables selection (D7.2) it also facilitates discrimination, while the lack of effective transparency enables undetected unjustified discrimination

2.2.3 Chapter 3: Legal issues

Keeping in mind the work done in deliverables 7.3 and 7.4 this chapter will focus on the applicability of data protection legislation (contribution of ICRI) to data provided by RFID applications within AmI environments, and to issues around liability (contribution of TILT), possibly extending to issues concerning criminal law and forensics (TILT).

Relevant issues at this point are:

- we should at least supply a survey of applicable legislation, referring to D7.3 and the first SWAMI-deliverable; if LBS is a forerunner of AmI and RFID is one of its enabling technologies it should be interesting to check the applicable legislation (like the ePrivacy Directive 2002/58/EC) and discern differences between LBS and AmI – relevant for the legal protection
- Data minimisation principle: explain the tensions between the data minimisation principle and RFID enhanced targeted servicing, LBS and AmI environments.

- PII: In which case, at what point is data collected PII? What happens to the applicability of the Data Protection Directive, if any (trivial) data (after being combined with other data) can produce (become) PII?Consent: Does data protection legislation protect against unrecognised readability of RFID-tags, especially relevant in the case of massive introduction of RFID for passive authentication? How should we prioritize enabling/disabling mechanisms and/or kill-command withdrawal of consent?
- Illegal data transfer and data laundering (reference to SWAMI) - due to the lack of effective transparancy – need legal protection; what is the role of the protection of databases by intellectual property rights in the lack of transparancy here?
- Privacy: (When) do people have a right to anonymity/pseudonymity? How does RFID related to the data minimisation principle, the finality principle and the principle of accuracy of data (reference to the technological chapter)?

- Discrimination: since profiling enables selection (D7.2) it also facilitates discrimination, while the lack of effective transparency enables undetected unjustified discrimination, which effective legal protection is available and what happens if decisions are taken on the basis of false information and if data are forwarded to third parties without knowledge of the data subject?
- Consent, privacy, discrimination, liability: at which point (under which conditions) should supplementation and/or modification and of tag data possible by the data reader (reference to the technological chapter)?
- Smart home (legal aspects, reference to the technological chapter): who is data controller in the smart home? If the rfid *system* includes online connections with service providers, are they data controllers and/or is the software provider data controller? To what extent can the user control the data?
- Liability: if we compare to liability issues in the case of PDA's (liability of the software provider for the design;, thinking in terms of a user mandate on the basis of a programmed will), the solutions that are sufficient in that case may not work in an AmI environment, due to the complexity and fuzzyness of the involved causal chains. Do we need to rethink conventional concepts of civil – and criminal - law (legal subjectivity, guilt, fault, representation, attribution of causality)?

2.2.4 Chapter 4: Social aspects

This chapter could be divided into three parts, containing (1) an exploration by IPTS and ICPP of possible social implications and relevant policy options (2) an integrated perspective on the technological, formal and informal aspects of RFID-related application in AmI environments and by LSE, and (3) an overview of academic sociological literature on RFID in relation to AmI and profiling by VUB.

Relevant issues at this point are:

- RFID seems to focus on the tracking of things. What impact could this entail on social interactions?

- acceptance of AmI and RFID will depend on trust and usability. Consumers don't seem to 'buy' the 'consumer focus narrative'; will the required paradigm shift towards AmI enabling technologies (RFID and other mobile identifications) occur and what could facilitate such a shift; should we appreciate the attempt to introduce RFID at gadget level facilitating wider dissemination and function creep instead of a well-informed consensus on extended use of RFID? Further elaboration of this issue, as presented in chapter 1.
- discussion of Jiang's 'minimum data asymmetry': ‘a privacy-aware system should minimize the asymmetry of information held between data owners and data collectors and data users, by (1) decreasing the flow of information from data owners to data collectors and users and (2) by increasing the flow of information from data collectors and users back to data owners’

2.2.5 Concluding chapter 5: Chances and risks of RFID applications in adaptive environments

This chapter should focus on summarising and linking the diversity of perspectives, detecting the most important findings in terms of opportunities and risks relating to RFID applications in adaptive environments. The editors could make this a joint venture, reconfiguring the mosaic of different disciplinary perspectives into a coherent picture.

3 Important issues and structure of planned report D7.7

3.1 Important issues

The slides underneath give an overview of the important issues which were proposed to be included into the deliverable 7.7 'AmI, RFID and Profiling'. The issues were discussed during the workshop.

The slides – and the updates of these slides - will be available on the internal portal, wp 7 section of the filemanager.


implications of enhanced robotics
usability
acceptance depends on trust and usability
consumer focus 'narrative'
required paradigm shift?
trust
acceptance depends on trust and usability
slow introduction at gadget level
privacy
function creep
presumes and produces profiling infrastructure
supplementation/modification of tag data by tag reader
categories of data stored
applicable legislation
data minimisation principle
finality principle
accuracy of data
2


LBS based on RFID location data
applicable legislation
ePrivacy Directive 2002/58/EC
automated real time adaptation
decisions taken on false information
data and profiles forwarded to third parties
who is data controller smart home
rfid system includes online connections with service providers, are they data controllers?
is the software provider data controller?
will the user control the data?
liability issue
comparison to liability issues PDA's: software provider, user (mandate)
programmed will (software designer/mandate user), not sufficient in AmI environment (complexity fuzzyness of causal chains)?
rethinking conventional concepts of civil – and criminal - law (legal subjectivity, guilt, fault, representation, attribution of causality)
facilitation of discrimination
profiling enables selection
lack of transparency enables undetected unjustified discrimination
illegal data transfer
data laundering
lack of transparency (protection of database by intellectual property rights)
3

3.2 Proposed structure of the document D7.7

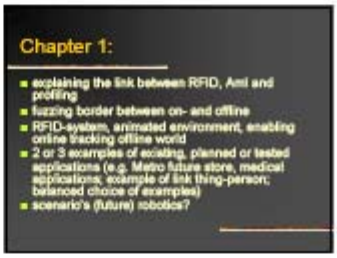
A first proposal of structuring the document was designed by the WP 7 leader, elaborating on the proposal made by Martin Meints of ICPP, it was discussed and amended during the workshop by all partners involved in the deliverable D7.7.

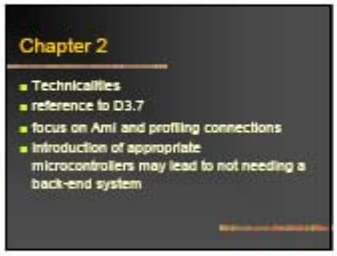
The slides underneath – including the updates of these slides - will be available on the internal portal, wp 7 section of the filemanager.

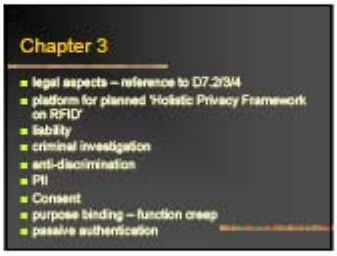

Structure of the report; division of tasks
FIDIS workshop D7.6
RFID-AmI-Profiling
20 January 2006

Timepath
15 March abstract
15 April 1st version contributors
1 May comments editors
15 May final version contributors
1 June final version report; internal review
15 June comments
1 July off to the Commission


Editors – internal reviewers

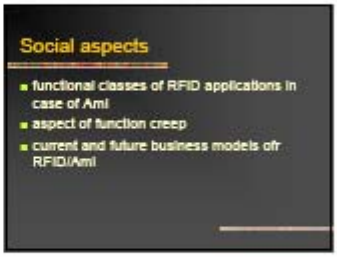

Chapter 1:
explaining the link between RFID, AmI and profiling
fuzzing border between on- and offline
RFID-system, animated environment, enabling online tracking offline world
2 or 3 examples of existing, planned or tested applications (e.g. Metro future store, medical applications; example of link thing-person; balanced choice of examples)
scenario's (future) robotics?


Chapter 2
Technicalities
reference to D3.7
focus on AmI and profiling connections
introduction of appropriate microcontrollers may lead to not needing a back-end system


Chapter 3
legal aspects – reference to D7.2/3/4
platform for planned 'Holistic Privacy Framework on RFID'
liability
criminal investigation
anti-discrimination
PII
Consent
purpose binding – function creep
passive authentication

1


Chapter 4


Social aspects
functional classes of RFID applications in case of Ami
aspect of function creep
current and future business models ofr RFID/Ami

2

4 Participants

1. Eleni Kosta	K.U.Leuven ICRI
2. Verena Vanessa Hafner	TUB DAI-Labor
3. Mark Gasson	Reading
4. Claudia Diaz	K.U.Leuven COSIC
5. Albin Zuccato	Karlstad University
6. Mina Deng	K.U.Leuven COSIC
7. Denis Royer	JWG Frankfurt University
8. Sabine Delaitre	IPTS
9. Anna Moscibroda	VUB
10. Michaël Vanfleteren	KULeuven ICRI
11. Ruth Halperin	LSE
12. Colette Cuijpers	TILT
13. Martin Meints	ICCP
14. Jan Möller	ICCP
15. .Mireille Hildebrandt	VUB
16. Soenens Els	VUB
17. . Wim Schreurs	VUB

5 Program

9.30: Welcome

9.30 – 10.00: Welcome and Coffee in room 4C306

10.00: Technological aspects

Technological aspects Physical properties, types, systems, security, areas of application How does this link to AmI and profiling?

ICCP 'RFID and Profiling'

Martin Meints, Jan Möller

10.00-10.20.

Expertise into:

- Technical RFID implementations and privacy legislational aspects of these implementations.

- Proposed structure for D3.7 and an AmI-related project called TAUCIS.

- Key issues of even simple RFID implementations are from our perspective:

    - Remote, unrecognised readability and thus the possibility to use RFID for passive authentication (lack of consent)

    - The link between object or/and subject and RFID

    - The need for in most cases centrally stored reference data and thus even in simple applications the basic database infrastructure for profiling

Proposal:

- chapter to define / describe the link between AmI, profiling and RFID. This should include 2 to 3 examples of existing, planned or tested solutions to elaborate the links between these topics and key issues of RFID as such. The Metro future store should be one of them, RFID and LBS is another important issue.

- In addition we probably need scenarios for the future (could probably be a question for Marc Gasson). This will definitely not be part of D3.7. We have to be careful with the technical chapter as this should not be a repetition of the planned D3.7. But basic aspects of RFID-implementation following probably the proposed TOC for D3.7 should be introduced and explained here to get an overview on the possibilities and limitations (including essential security problems) of this technology. The focus should be kept on AmI-related applications. I think we are pretty free in the legal chapter, but we should keep the results from D7.3 and D7.4 in mind. This chapter could as well serve as a platform for the planned "Holistic Privacy Framework on RFID".

- Essential aspects are

(1) purpose for data processing (who is in control of the AmI-environment, for what purpose it is being used?),

(2) legal aspects of passive authentication (also relevant for behavioural biometrics) and

(3) questions concerning consensus for transfer and processing of personal

IPTS prospects

Sabine Delaitre

10.20 -10.40

Proposal / Expertise:

- General RFID information on description of different classes of RFID and an analysis on the differences among them referring to infrastructure required, types of applications, operating environment limitations, need for security, cost/return on investment, and level of cooperation with other stakeholders

- Overview of technologies which when combined with RFID tags may enhance the use and adoption of RFID in the European Information Society

- Typology of RFID usage and some scenarios for its illustration

- Standards and discussion on integration, on implications, proc/cons, etc

DAI-Labor TUB, 'Context extension for mobile robots with RFID'

Vanessa Varena Hafner

10.40 – 11.00

- The Mobile Robot Project aims at enhancing the sensory capabilities of a mobile robot which is equipped with an omnidirectional camera and a compass with an RFID reader. The mobile robot is exploring its environment and creating a cognitive map of this environment based on place nodes, inspired by place cells measured in rat brains.
- we are planning to extend the sensory capabilities of the robot with an RFID reader, and have a tagged environment. Tags can be attached to the floor, doors, different static and flexible objects, other robots and humans. They can provide the robot with additional contextual information about its current position in relation to the environment and wit additional information about objects and other agents.
- Our expertise is in the fields of robotics, Artificial Intelligence, smart interfaces and devices, and we would like to discuss the abovementioned project in relation with privacy and security aspects as well s risks and possibilities of these novel devices.

11.00: Coffee break

11.15: Technological aspects (bis)

Reading 'Embedding Intelligence: Emerging applications of RFID' with a core focus on implantable apps.

Mark Gasson

11.15 – 11.35

A host of implications are associated with the continuing introduction of disparate RFID applications. These include:

- **Usability**: While historically RFID applications have been industrial in nature, continuingly new consumer-focussed applications have found some degree of acceptance. However, the grandiose visions of technologists have to date found little consumer acceptance, perhaps due to the paradigm shift required in people's long established relationship with technology.

- **Trust**: No single technology will become established in the consumer market without the trust of its target audience. Currently, few people are aware of the issues surrounding the use of RFID tags, and as such the slow introduction of the technology in 'gadget' level devices allows for it to be subtly introduced into the public consciousness. The subsequent familiarity with the technology makes it more difficult to later comprehend the dangers of mass rollout, with the classic argument 'I already have some of these, why will another one hurt?'

- **Privacy**: One of the biggest dangers associated with RFID technologies is the issue of 'function creep'. Whilst ironically profiling is hailed as one of the greatest advantages of this technology, allowing for the long purported AmI environments, it is exactly this issue which may prove to be its downfall.

11.35: Legal Aspects

Legal aspects Existing legal framework (Data Protection, ePrivacy Directives) How does this link to AmI and profiling?

ICRI-Leuven 'Privacy aspects of RFID in AmI and profiling'.

Eleni Kosta

11.35 – 11.55

- RFID tags can be embedded in objects that are closely related to a person and in this way they enable her tracking and tracing. Besides that, they can also be embedded directly in a

person and allow her real and ubiquitous tracing and tracking (hereinafter we shall call the person who is related to the RFID tag or on whom the RFID tag is embedded as 'user').

- Some of the main data protection and privacy concerns

  - specific kinds of RFID tags allow the supplementing and modification of the 'tag data' by the tag reader.

  - the surreptitious, unwanted individual tracking performed by unauthorised access to the tag's disclosed information or memory content.

ICRI can contribute to

  - the description of the existing legal framework that could be applied on RFID technology, differentiating when necessary between the several types of RFID tags .

  - Focus on the categories of data that can be stored on and collected from an RFID tag and the general rules according to which the data should be collected and processed (data minimisation principle, finality principle, accuracy of the data etc.).

  - Data stored on the RFID tag that are used for the location of the user shall be considered as 'location data' enabling Location Based Services. In these cases the specific provisions of the ePrivacy Directive (2002/58/EC) shall apply.

  - the notion of 'consent' in relation with the RFID tags and the differences between the 'enabling/disabling mechanism' and the 'kill-command' as means of withdrawal of the consent.

5.1.1 TILT's expertise and relevant issues

Colette Cuijpers.

11.55 – 12.15

- TILT's expertise covers a wide range of topics related to developments in ICT, biotechnology, and other technologies. These developments are studied in the contexts of important domains of the developing knowledge society, such as e-government, e-commerce, e-health, ICT regulation, biotechnology and nanotechnology, privacy, identity management, e-signatures, biometrics, cybercrime, security, intellectual property rights, citizenship and governance, globalisation, Europeanisation, and ethics.

- A key feature of the institute's research and educational programmes is the interaction between legal, public administration and ethics experts, between law, regulation, and governance, and between legal, technical, and social perspectives. Our research programme is called 'Regulation in the Information Society: The Interaction of Law, Technology (in Particular ICT), and Social Structures'. Attention is given to various dilemmas in balancing societal interests (security versus privacy; freedom versus ownership of information; etc.). Using the research results from the perspectives of law, technology, and social values and relationships, building blocks are formulated for a normative framework for the regulation of

technology. As you can see, societal problems related to the use of AmI, RFID and profiles fit perfectly within this programme and is therefore high on our agenda.

Regarding the important issues we think the FIDIS report on RFID, AmI and profiling should deal with, we have formulated several research questions.

- Identification is necessary. What kind of identification is required for AmI, and what does this mean for the privacy of the individual?
- (How) can one object to identification? How does identification relate to a right to anonymity or at least pseudonymity? Are pseudonyms sufficient in relation to the functioning of AmI?
- What is the relation between the combination of a pseudonym as a handle (identifier) to a data set and a profile, which also is a data set?
- When exactly is data collected in the sphere of Ami Personally Identifiable Information (PII)? Has it always been PII, or is there a moment in time when it becomes PII by association?
- What about group identification in the case of group profiling? Even though an individual in a group profile cannot be identified, the identification as a someone belonging to a certain group can have unwanted consequences.
- Faults within a profile or misinterpretations by AmI sensors can lead to an incorrect representation of a person or her preferences or characteristics and therefore to a 'false' identity, next to her true identity. Can legal decisions be based on both?
- What is identity? How much information constitutes an identity and where does the boundary lie with mere characteristics? What if the data constituting a person's identity is not embedded in a file, but is composed of fragments in an open network environment, or from different sensors, jointly to be perceived as an identity, or at least as a set of data on the basis of which decisions are made? Is virtual identity the same as identity in the real world? Is the concept of identity as used in our data protection laws suitable to accommodate for virtual identities that do not have to relate to existing natural persons?
- Who is the data controller in the case of in-house Ami? The user herself?
- And who is the data controller if different environmental sensors communicate amongst each other and with sensors on different individuals, that in turn communicate with each other? Is there always a central server involved?

A different approach we could take regarding AmI is liability issues. Again we could use (worst case) scenarios in which decisions taken by AmI lead to unwanted and damageable situations for the AmI user. In this respect the question arises whether liability issues in the field of AmI are the same as those relating to (intelligent) agents. Probably other (legal) problems arise due to different parties and techniques involved in AmI. The use of an agent is usually confined to a more or less known group of involved parties who can create their own legal settings by contracts, while the concept of a programmed will is often sufficient to handle problems. In an AmI environment, which in it’s flourishing days might entail hundreds of sensors in one's direct environment, not only communicating with the user, but also influencing each other, responsibilities and causal chains are far less clear. Contractual solutions are not possible as responsible ‘persons’ are not detectable and a programmed will is not that obvious. The lack of transparency also forms a problem for tort law. So, the question arises whether traditional law can cope with liability issues arising due to a large scale

introduction of AmI? More in general, does the overall and interacting nature of AmI come into conflict with traditional concepts on which our data protection and civil laws are vested?

VUB: overview findings Swami

Anna Moscibroda

12.15 –12.35

SWAMI project (Safeguards in the World of Ambient Intelligence) aims to identify and analyse the social, economic, legal, technological and ethical problems and issues related to identity, privacy and security which may emerge in Ambient Intelligence environment. In order to take into account the major trends in the field, existing AmI projects and studies have been revised. SWAMI consortium also composed and analysed and the "dark" scenarios, the aim of which was to expose key socio-economic, legal, technological and ethical risks and vulnerabilities related to issues such as identity, privacy and security that may emerge from the deployment of AmI technologies and services, among other also in relation to the RFID and profiling. Consortium has identified the umber of vulnerabilities relating to AmI. RFID and profiling brings special attention to the issues like privacy protection, consequences of inadequate profiling and dependency, digital divide and discrimination.

The next step of the work is to define and study various policy options, which could serve as safeguards and privacy-enhancing mechanisms.

12.30: Lunch

13.00: Social Aspects

Social aspects Interoperability, privacy, mobile identity, economic aspects How does this link to AmI and profiling?

KU 'Privacy enhancing and secure solutions for RFID tags in the supply chain'

Albin Zaccato

13.00- 13.20

- RFID in general, tags in packages

- privacy problems

- PETS, holistic solutions

- Link to the work package 12 proposals of the third work plan.

5.1.2 GUF 'Mobility, Location based services and economic issues'

Denis Royer

13.20 – 13.40

- Mobility,

- LBS and link to AmI

- Economic issues

- Importance of LBS to AmI.

13.40: Overview literature

Overview literature A first outline will be presented of the issues detectable in literature on RFID, AmI and profiling, and of the extent to which different disciplinary perspectives are taken into account.

VUB 'Overview of the literature collection on AmI, RFID, Profiling and Identity.'

Els Soenens

13.40 - 14.00

The presentation will explore my individual collection of literature on AmI, RFID, Profiling and/or Identity. The collection tried to cover a range of various perspectives, from the sociological, economical, and ethical to the technical and the legal, as well as combinations of these perspectives. The collection could function as a starting point for an elaborated, centralised collection of relevant FIDIS resources which would have the advantage of taking down the walls between the different work packages and disciplines.

As an introduction and without claiming its value as a database, the methodology used to set up the collection of literature will be revealed. Secondly, based on data filtering application in some general tendencies of the collection are presented.

Believing the AmI vision can only succeed when overcoming its major challenges by way of holistic solutions, the papers covering a multi perspective point of view on AmI are of special interest. Limited by the time constraints of this presentation, the emphasis is on the user centric claim of the AmI vision.

14.00: Discussion and selection of relevant issues

Discussion and selection of relevant issues The relevant transversal issues detected during the presentations will be discussed and prioritised.

The slides of the relevant issues made prior to the workshop are presented in the section Important issues 3.1.

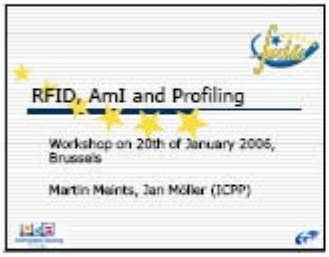
15.00: Coffee break

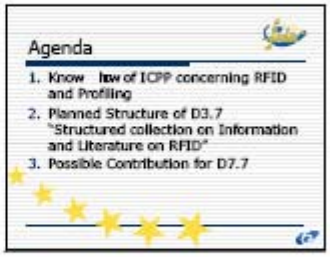
15.15: Discussion on structure of the report D7.7 & division of tasks

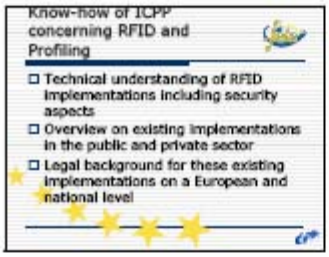
Discussion on structure of the report D7.7 & division of tasks Defining the structure of the document, on the basis of the transversal issues. Selection of editors and deciding who contributes in which way to the document.

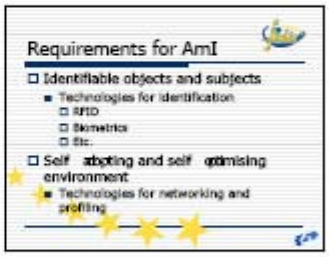
The slides of the structure of the report made prior to the workshop are presented in the section 3.2 Proposed structure of the document D7.7.

6 Annex I: Slides of the presentations

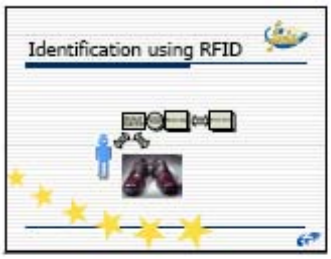


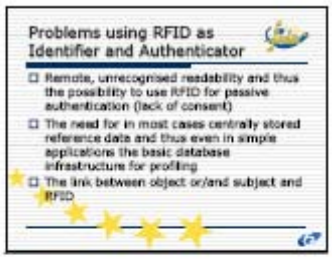


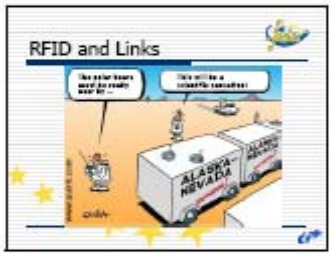




1

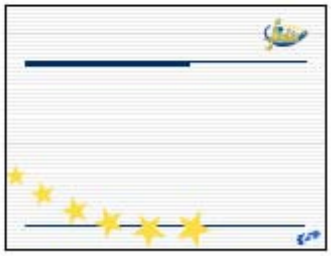

Identification using RFID


Problems using RFID as Identifier and Authenticator
Remote, unrecognised readability and thus the possibility to use RFID for passive authentication (lack of consent)
The need for in most cases centrally stored reference data and thus even in simple applications the basic database infrastructure for profiling
The link between object or/and subject and RFID


RFID and Links
ALASKA
NEVADA

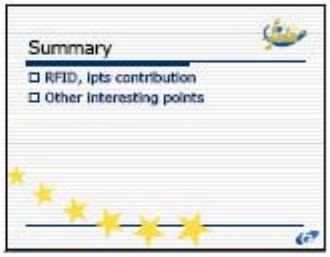

RFID and Links (cont.)

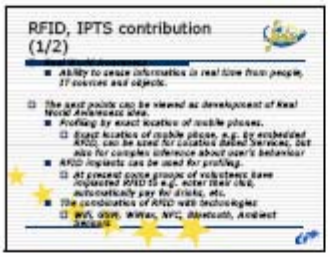

Thank you for your attention!
?

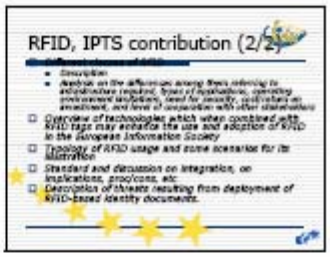


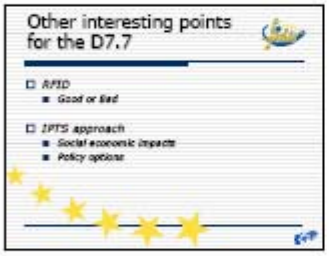
2


D7.7 outline:
AmI, RFID, profiling


Summary
RFID, Ipts contribution
Other interesting points


RFID, IPTS contribution (1/2)


RFID, IPTS contribution (2/2)

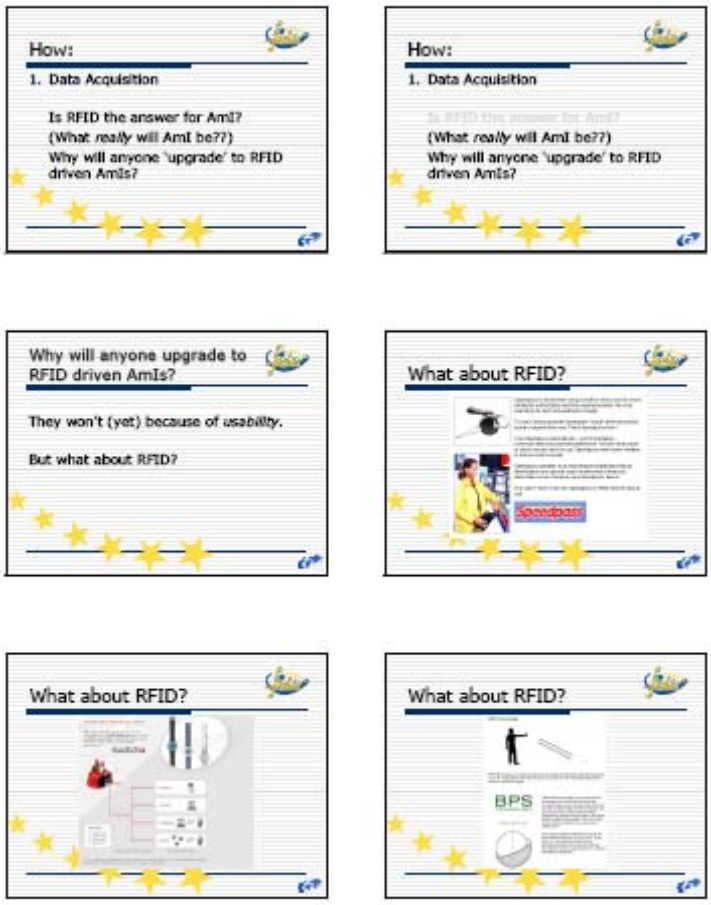

Other interesting points for the D7.7
RFID
Good or Bad
IPTS approach
Social economic impacts
Policy options


Thank you

3

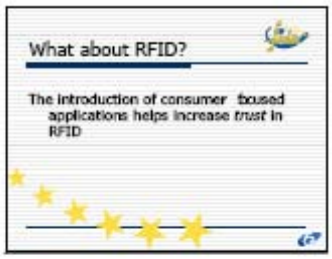

Phidgets RFID Kit
tagging objects and agents
RFID reader
RFID tag
RFID tag
RFID tag
RFID tag
What else could be tagged?
"After the fish are served in restaurant, dishes are served to customers together with the 2D barcode. Customers can view the encoded information using their mobile phones before, during, or after enjoying the dishes."
Privacy Issues
Who can access the information?
What is tagged?
Is cloning possible?
What would be the dangers?
"Report on AmI, Profiling and RFID"
WP7 – D7.6 / D7.7
Dr Mark Gasson
University of Reading

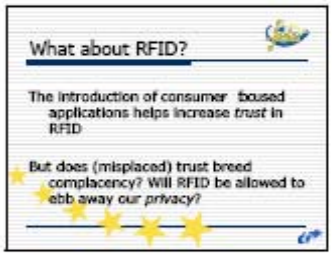
5

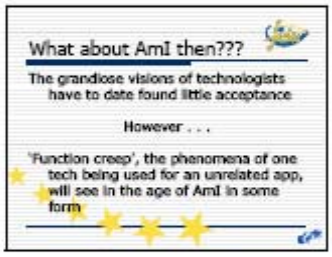

How:
1. Data Acquisition
Is RFID the answer for AmI?
(What *really* will AmI be??)
Why will anyone 'upgrade' to RFID driven AmIs?
How:
1. Data Acquisition
(What *really* will AmI be??)
Why will anyone 'upgrade' to RFID driven AmIs?
Why will anyone upgrade to RFID driven AmIs?
They won't (yet) because of *usability*.
But what about RFID?
What about RFID?
Speedpass
What about RFID?
What about RFID?
BPS

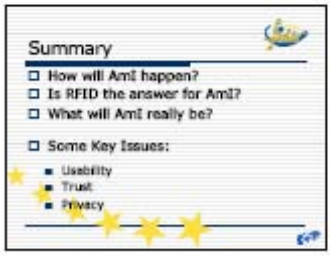
7


What about RFID?


What about RFID?
The introduction of consumer focused applications helps increase *trust* in RFID

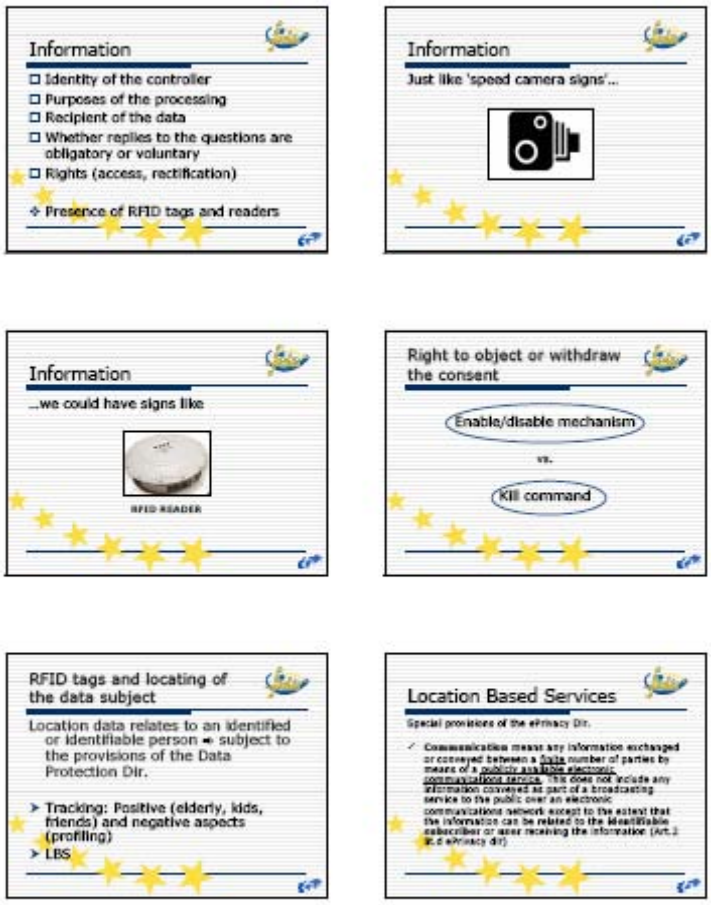

What about RFID?
The introduction of consumer focused applications helps increase *trust* in RFID
But does (misplaced) trust breed complacency? Will RFID be allowed to ebb away our *privacy*?


What about AmI then???
The grandiose visions of technologists have to date found little acceptance
However . . .
'Function creep', the phenomena of one tech being used for an unrelated app, will see in the age of AmI in some form


Summary
How will AmI happen?
Is RFID the answer for AmI?
What will AmI really be?
Some Key Issues:
Usability
Trust
Privacy


Questions and Answers
?

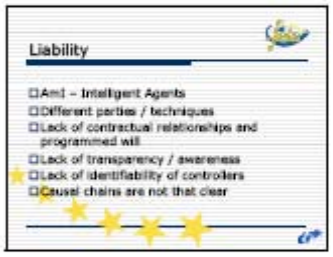
8

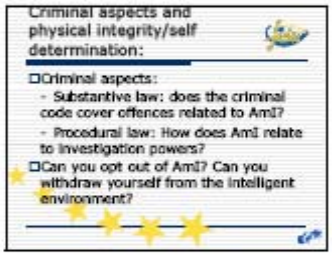

Information
Identity of the controller
Purposes of the processing
Recipient of the data
Whether replies to the questions are obligatory or voluntary
Rights (access, rectification)
Presence of RFID tags and readers
Information
Just like 'speed camera signs'...
Information
...we could have signs like
RFID READER
Right to object or withdraw the consent
Enable/disable mechanism
vs.
Kill command
RFID tags and locating of the data subject
Location data relates to an identified or identifiable person → subject to the provisions of the Data Protection Dir.
Tracking: Positive (elderly, kids, friends) and negative aspects (profiling)
LBS
Location Based Services
Special provisions of the ePrivacy Dir.

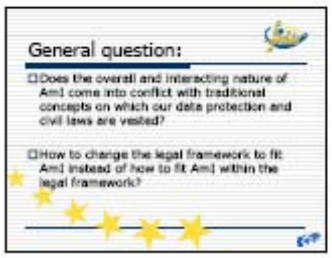
11

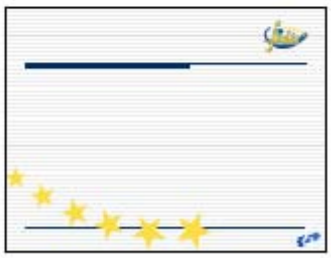

Privacy and data protection I:
(Passive) authentication
Consent / withdrawal of consent
Function creep
modification tag data by tag reader
Unauthorized access
Application of data protection rules to (different kinds of) RFID tags
(define and study various policy options, which could serve as safeguards and privacy enhancing


Privacy and data protection II:
PII
False identity and true identity, applicability of data protection rules and legal decisions
Who is the data controller?
Data protection and group profiling (D7.2 – D7.5)


Liability
AmI – Intelligent Agents
Different parties / techniques
Lack of contractual relationships and programmed will
Lack of transparency / awareness
Lack of identifiability of controllers
Causal chains are not that clear


Criminal aspects and physical integrity/self determination:
Criminal aspects:
- Substantive law: does the criminal code cover offences related to AmI?
- Procedural law: How does AmI relate to investigation powers?
Can you opt out of AmI? Can you withdraw yourself from the intelligent environment?


General question:
Does the overall and interacting nature of AmI come into conflict with traditional concepts on which our data protection and civil laws are vested?
How to change the legal framework to fit AmI instead of how to fit AmI within the legal framework?



13


SWAMI: Safeguards in a World of Ambient Intelligence
SWAMI- presentation of the project and its first results


SWAMI: Safeguards in a World of Ambient Intelligence
Objective
The project aims to identify and analyse the
• Social, economic, legal, technological, and ethical issues
• Related to identity, privacy and security
• Which may emerge in Ambient Intelligence (AmI) environments.

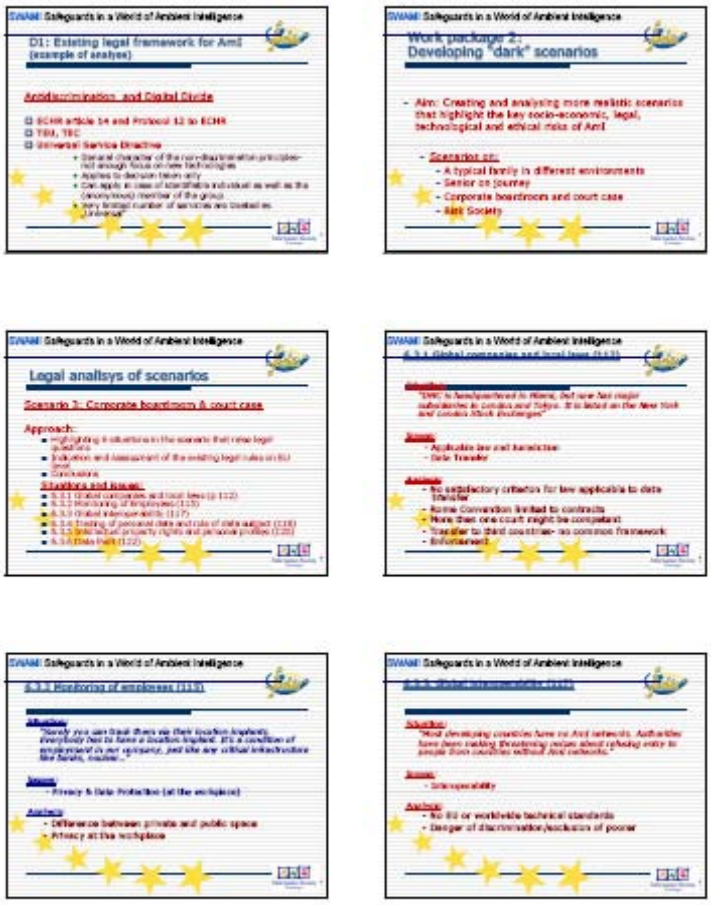

SWAMI: Safeguards in a World of Ambient Intelligence
Participants
Multidisciplinary consortium
Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany.
Technical Research Center of Finland, VTT Electronics, Oulu, Finland.
European Commission/Joint Research Center-Institute for Prospective Technological Studies, Seville, Spain.
Free University Brussel, Center for Law,Science, Technology and Society Studies, Belgium.
Trilateral Research & Consulting, London, United Kingdom


SWAMI: Safeguards in a World of Ambient Intelligence
Work packages
- Work package 1 (WP1): State of the art review of existing AmI projects, studies, scenarios and roadmaps (July 2005)
- Work package 2 (WP2): Developing "dark" (adverse) scenarios (November 2005)
- Work package 3 (WP3): Developing legal and policy options which could serve as safeguards and privacy-enhancing mechanisms for Ambient Intelligence (ongoing)

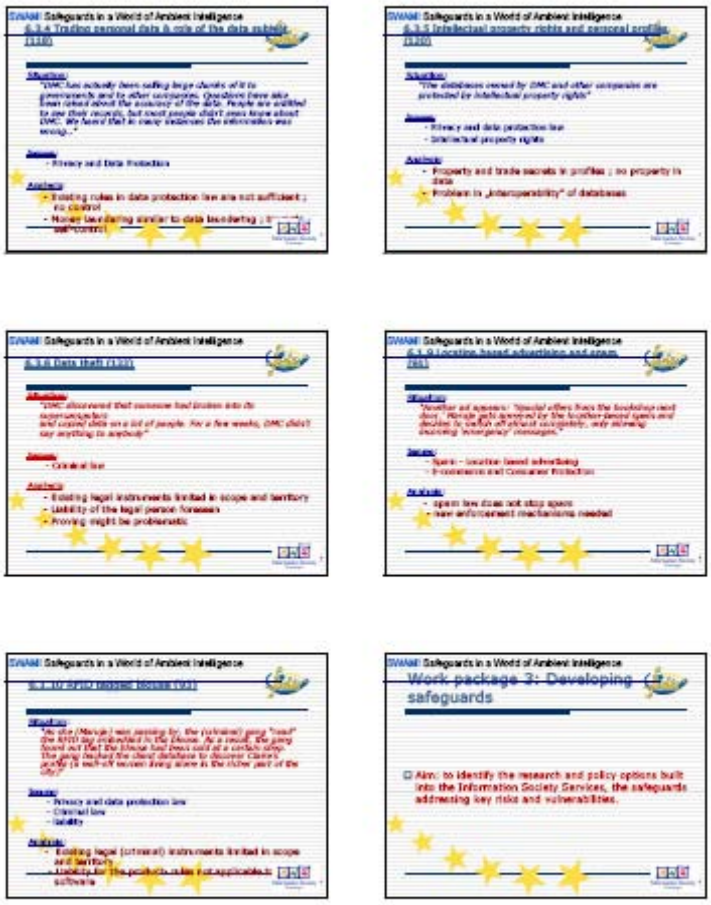

SWAMI: Safeguards in a World of Ambient Intelligence
Work package 1: A state-of-the-art
- Deliverable D1: The brave new world of ambient intelligence: A state-of-the-art review (July 2005)
- AmI research in Europe, the United States and Japan
- Analysis of (existing) ambient intelligence scenarios
- Existing legal framework for AmI
- Summary and first conclusions


D1: Existing legal framework for AmI
Subject matters:
• Privacy and Data Protection
• Intellectual Property Rights
• E-commerce and Consumer Protection
• Torts and Liability
• I.C.T. Law
• Criminal Law
• Antidiscrimination law
• Jurisdiction and Applicable Law

14


SWAMI: Safeguards in a World of Ambient Intelligence
D1: Existing legal framework for AmI (example of analyse)
Anti-discrimination and Digital Divide
SWAMI: Safeguards in a World of Ambient Intelligence
Work package 2: Developing "dark" scenarios
- Aim: Creating and analysing more realistic scenarios that highlight the key socio-economic, legal, technological and ethical risks of AmI
- Scenarios on:
- A typical family in different environments
- Senior on journey
- Corporate boardroom and court case
- Alert Society
SWAMI: Safeguards in a World of Ambient Intelligence
Legal analysys of scenarios
Scenario 3: Corporate boardroom & court case
Approach:
SWAMI: Safeguards in a World of Ambient Intelligence
Applicable law and Jurisdiction
Data Transfer
- No satisfactory criterion for law applicable to data transfer
- Rome Convention limited to contracts
- More than one court might be competent
- Transfer to third countries- no common framework
- Enforcement
SWAMI: Safeguards in a World of Ambient Intelligence
6.3.3 Monitoring of employees (113)
Privacy & Data Protection (at the workplace)
- Difference between private and public space
- Privacy at the workplace
SWAMI: Safeguards in a World of Ambient Intelligence
- Interoperability
- No EU or worldwide technical standards
- Danger of discrimination/exclusion of poorer

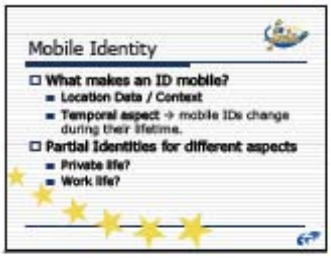
15


SWAMI: Safeguards in a World of Ambient Intelligence
Work package 3: Developing safeguards
Aim: to identify the research and policy options built into the Information Society Services, the safeguards addressing key risks and vulnerabilities.

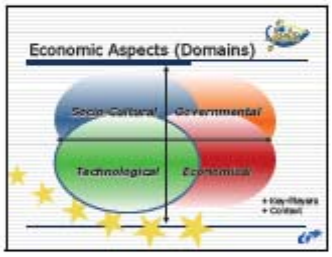
16


SWAMI: Safeguards in a World of Ambient Intelligence
Threats and Vulnerabilities
Examples of (relevant) identified threats and/or vulnerabilities:
Surveillance (i.e. automated decision)
Spamming and location based advertising
Digital Divide and discrimination
Inadequate profiling/incomplete profiling
Dependency (i.e. automated decisions)
Data laundering
Malicious attacks
etc.
SWAMI: Safeguards in a World of Ambient Intelligence
D1: Existing legal framework for AmI
"Mobility, LBS, economic issues"
WP7 Workshop on RFID, AmI and Profiling
Denis Royer
Agenda
The work of WP11
Location Based Services
Questions and Answers
WP11: Mobility and Identity
D11.1: Identification and description of the term 'mobile identity'.
D11.3: Evaluation of economic aspects of mobile identity management and identification of the critical success factors.
D11.2: Evaluation of Location Based Services (LBS) from different perspectives (e.g. Technology, Profiling, Identification & Privacy).

17


Mobile Identity
What makes an ID mobile?
Location Data / Context
Temporal aspect → mobile IDs change during their lifetime.
Partial Identities for different aspects
Private life?
Work life?


Economic Aspects
A variety of different aspects have a impact on the economic aspects
Aspects have a high level of interdependencies.
Questions to be answered:
Identification of the key-players.
How to evaluate intangible factors (security, privacy, etc.)?
Impact of other domains on economy?
Is it possible to find a unified solution for the evaluation of economic aspects?

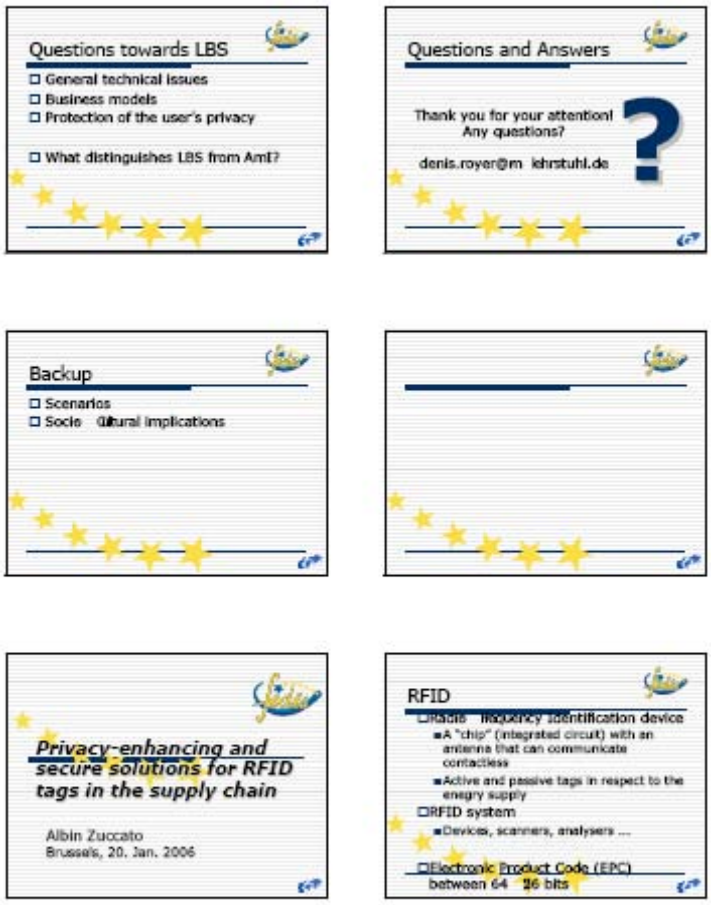

Economic Aspects (Domains)
Socio-Cultural
Governmental
Technological
Economical
+ Key-Players
+ Context


Economic Aspects
Diffusion of Innovations
What makes a technology successful?
How it gets accepted in the market?
Stages of Adoption:
Awareness, interest, evaluation, trial, and adoption
Technology Acceptance Model
Perceived usefulness
Perceived ease-of-use
Price of Convenience

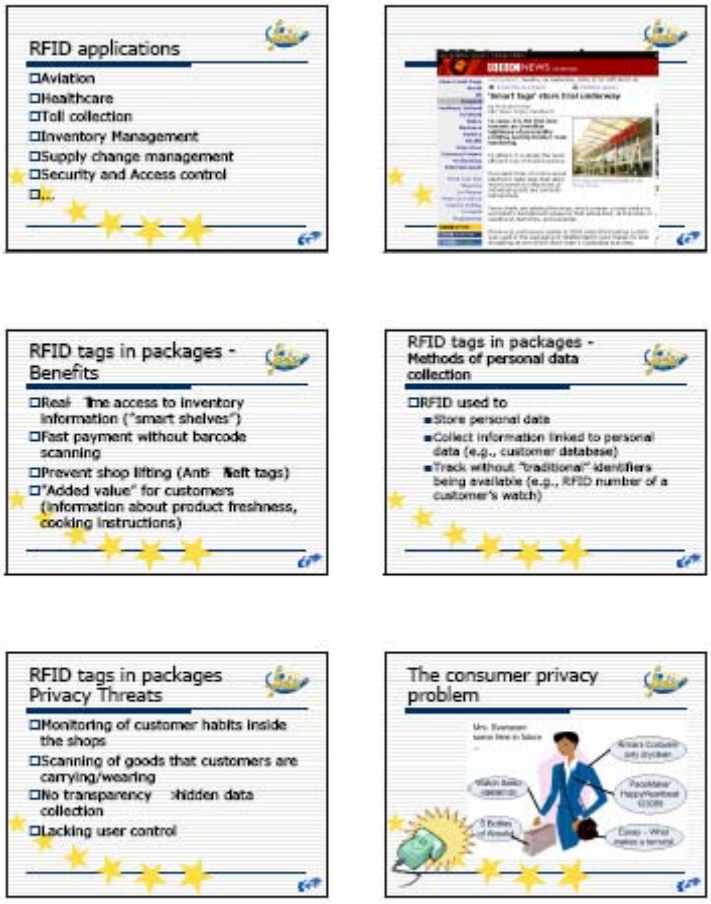

Diffusion of Innovations


Location Based Service (LBS)

18

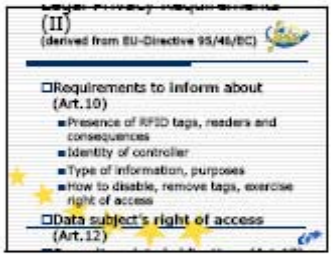

Questions towards LBS
General technical issues
Business models
Protection of the user's privacy
What distinguishes LBS from AmI?
Questions and Answers
Thank you for your attention!
Any questions?
denis.royer@m ehrstuhl.de
Backup
Scenarios
Socio cultural implications
Privacy-enhancing and secure solutions for RFID tags in the supply chain
Albin Zuccato
Brussels, 20. Jan. 2006
RFID
A "chip" (integrated circuit) with an antenna that can communicate contactless
Active and passive tags in respect to the energy supply
RFID system
Devices, scanners, analysers ...
Electronic Product Code (EPC)
between 64 96 bits

19

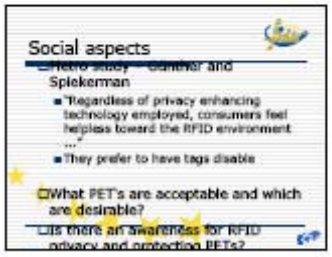

RFID applications
Aviation
Healthcare
Toll collection
Inventory Management
Supply change management
Security and Access control
...
RFID tags in packages - Benefits
Real Time access to inventory information ("smart shelves")
Fast payment without barcode scanning
Prevent shop lifting (Anti Theft tags)
"Added value" for customers (information about product freshness, cooking instructions)
RFID tags in packages - Methods of personal data collection
RFID used to
Store personal data
Collect information linked to personal data (e.g., customer database)
Track without "traditional" identifiers being available (e.g., RFID number of a customer's watch)
RFID tags in packages Privacy Threats
Monitoring of customer habits inside the shops
Scanning of goods that customers are carrying/wearing
No transparency hidden data collection
Lacking user control
The consumer privacy problem
20


Holistic solution required
Legal Requirements
requires
Economic aspects
has
PET
imply
Social aspects


Legal Privacy Requirements (I)
(derived from EU-Directive 95/46/EC)
• Legal ground: informed consent (Art. 7 EU Directive)
• Purpose specification and purpose binding (Art. 6 I b)
• Data minimization (Art. 6 I c, Art. 7)

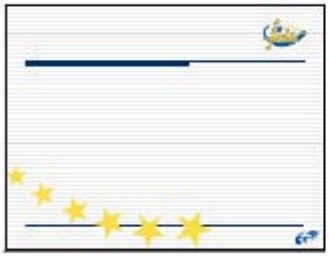

(II)
(derived from EU-Directive 95/46/EC)
Requirements to inform about (Art.10)
Presence of RFID tags, readers and consequences
Identity of controller
Type of information, purposes
How to disable, remove tags, exercise right of access
Data subject's right of access (Art.12)

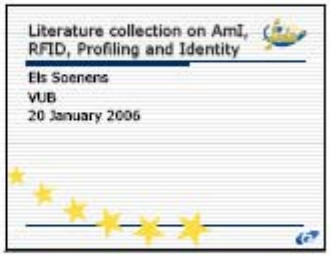

PET's (& Security)
Privacy Enhancing Technologies:
Killing tags at point of sale
Tag passwords and pseudonyms
Selective Blocker tags
RFID proxies
Privacy-enhanced identity management solutions
Security controls
Authentication, tag passwords, encryption,...

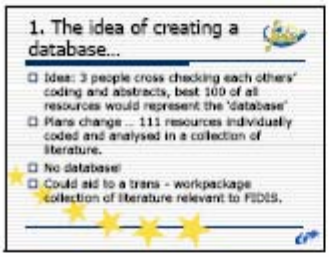

Social aspects
Spiekerman
"Regardless of privacy enhancing technology employed, consumers feel helpless toward the RFID environment ..."
They prefer to have tags disable
What PET's are acceptable and which are desirable?

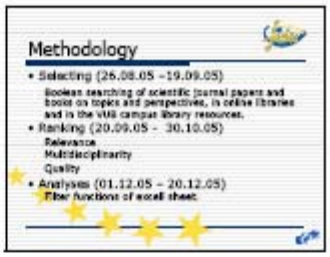

Economic aspects
What are the benefits for customers/suppliers to have RFID pets?
What are the costs for customers/suppliers to have RFID pets?
Are there other protection mechanisms?

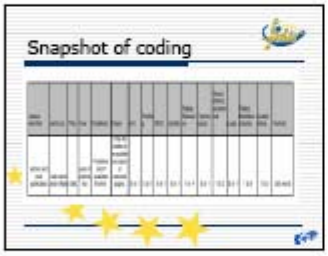
21

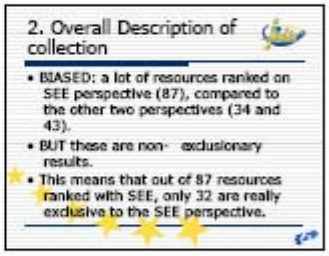



Literature collection on AmI, RFID, Profiling and Identity
Els Soenens
VUB
20 January 2006

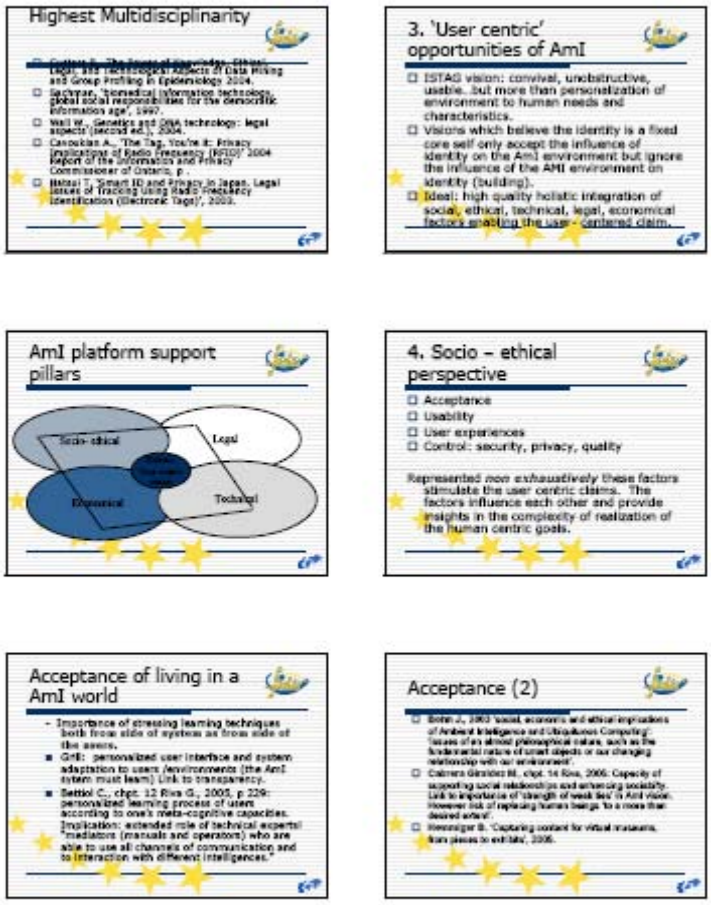

1. The idea of creating a database...
Idea: 3 people cross checking each others' coding and abstracts, best 100 of all resources would represent the 'database'
Plans change ... 111 resources individually coded and analysed in a collection of literature.
No database!
Could aid to a trans - workpackage collection of literature relevant to FIDIS.


Methodology
Selecting (26.08.05 -19.09.05)
Boolean searching of scientific journal papers and books on topics and perspectives, in online libraries and in the VUB campus library resources.
Ranking (20.09.05 - 30.10.05)
Relevance
Multidisciplinarity
Quality
Analyses (01.12.05 - 20.12.05)
Filter functions of excell sheet

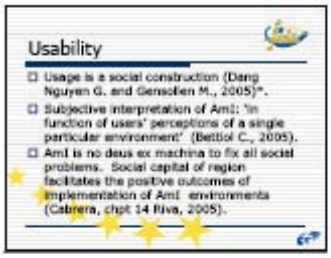

Snapshot of coding


2. Overall Description of collection
BIASED: a lot of resources ranked on SEE perspective (87), compared to the other two perspectives (34 and 43).
BUT these are non- exclusionary results.
This means that out of 87 resources ranked with SEE, only 32 are really exclusive to the SEE perspective.

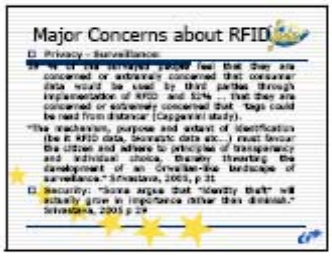
22

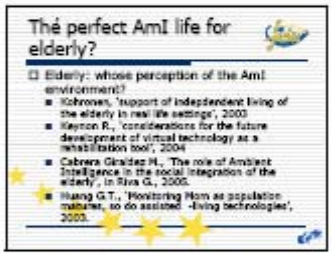

Highest Multidisciplinarity
3. 'User centric' opportunities of AmI
ISTAG vision: convival, unobstructive, usable.. but more than personalization of environment to human needs and characteristics.
Visions which believe the identity is a fixed core self only accept the influence of identity on the AmI environment but ignore the influence of the AMI environment on identity (building).
Ideal: high quality holistic integration of social, ethical, technical, legal, economical factors enabling the user - centered claim.
AmI platform support pillars
Socio- ethical
Legal
Technical
4. Socio – ethical perspective
Acceptance
Usability
User experiences
Control: security, privacy, quality
Represented non exhaustively these factors stimulate the user centric claims. The factors influence each other and provide insights in the complexity of realization of the human centric goals.
Acceptance of living in a AmI world
Acceptance (2)

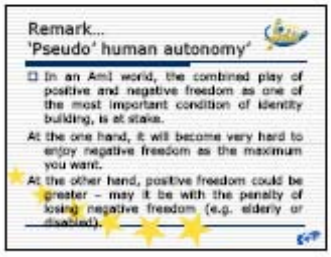
23


Usability
Usage is a social construction (Dang Nguyen G. and Genssollen M., 2005)".
Subjective interpretation of AmI: 'in function of users' perceptions of a single particular environment' (Bettiol C., 2005).
AmI is no deus ex machina to fix all social problems. Social capital of region facilitates the positive outcomes of implementation of AmI environments (Cabrera, chpt 14 Riva, 2005).


User experiences: need for scientific social research
"creative misuse" Di Duca D. , Van Hellvert J. "User Experience of Intelligent Buildings; A User- Centered Research Framework".*
Bernhaupt R., 'user experiences as missing link in multimodal interfaces for Ambient intelligence environments', 2004.
Schlosser, "So how do people really use their handheld devices? An interactive study of wireless technology use", 2002.
Rutledge M.G., 'Ambient intelligence, changing forms of human-computer interaction and their social implications', 2004.

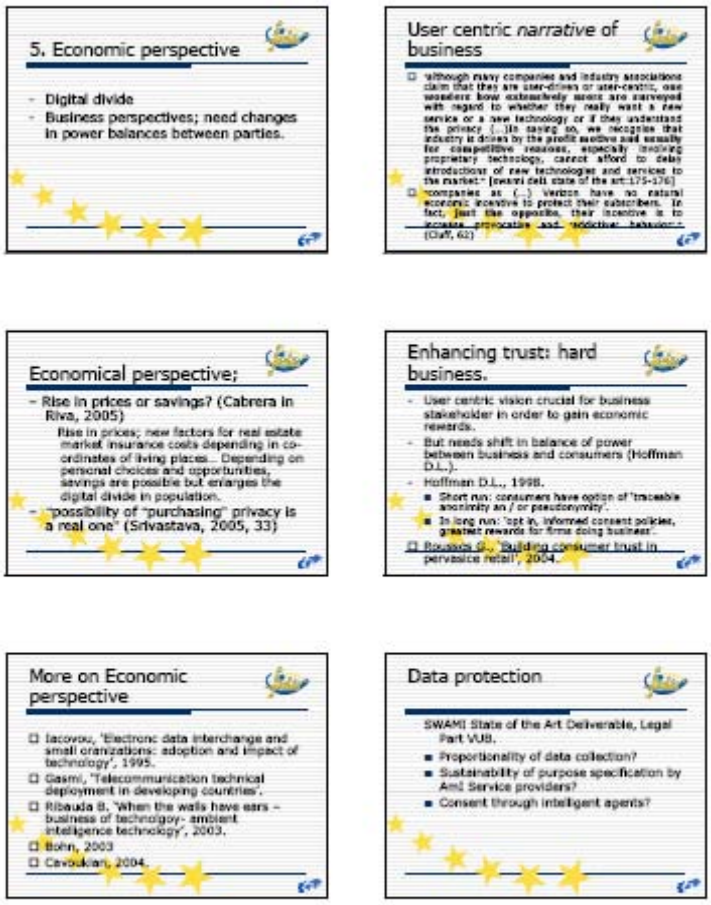

Major Concerns about RFID
Privacy – Surveillance:
"the machanism, purpose and extent of identification (be it RFID data, biometric data etc...) must favour the citizen and adhere to principles of transparency and individual choice, thereby thwarting the development of an Orwellian-like landscape of surveillance." Srivastava, 2005, p 31
Security: "Some argue that "identity theft" will actually grow in importance rather than diminish." Srivastava, 2005 p 29


Thé perfect AmI life for elderly?
Elderly: whose perception of the AmI environment?
Kohrouen, 'support of independent living of the elderly in real life settings', 2003
Keynon R., 'considerations for the future development of virtual technology as a rehabilitation tool', 2004
Cabrera Giraldez M., 'The role of Ambient Intelligence in the social integration of the elderly', in Riva G., 2005.
Huang G.T., 'Monitoring Mom as population matures, so do assisted -living technologies', 2003.


Remark...
'Pseudo' human autonomy'
In an AmI world, the combined play of positive and negative freedom as one of the most important condition of identity building, is at stake.
At the one hand, it will become very hard to enjoy negative freedom as the maximum you want.
At the other hand, positive freedom could be greater – may it be with the penalty of losing negative freedom (e.g. elderly or disabled).


Enhanced trust through:
Informed Consent; trust control and privacy (van der Geest T., 2005).
Principle of minimum asymmetry based on social science research on information asymmetry. See also work of Noerlof and Berg. (Berg V. 'elegant privacy – decentralised information space...', 2003, p 2).
Social contract enacted in the context of a cooperative relationship built on trust', more than economic (ie is data for commercial benefits. (Hoffman D.L., 1999).

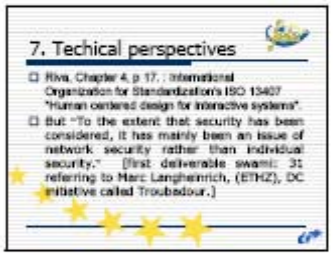
24


5. Economic perspective
- Digital divide
- Business perspectives; need changes in power balances between parties.
User centric narrative of business
Economical perspective;
– Rise in prices or savings? (Cabrera in Riva, 2005)
Rise in prices; new factors for real estate market insurance costs depending in co-ordinates of living places... Depending on personal choices and opportunities, savings are possible but enlarges the digital divide in population.
– "possibility of "purchasing" privacy is a real one" (Srivastava, 2005, 33)
Enhancing trust: hard business.
- User centric vision crucial for business stakeholder in order to gain economic rewards.
- But needs shift in balance of power between business and consumers (Hoffman D.L.).
- Hoffman D.L., 1998.
Short run: consumers have option of 'traceable anonimity an / or pseudonymity'.
In long run: 'opt in, informed consent policies, greatest rewards for firms doing business'.
Rousseau G., 'Building consumer trust in pervasive retail', 2004.
More on Economic perspective
Iacovou, 'Electronic data interchange and small oranizations: adoption and impact of technology', 1995.
Gasmi, 'Telecommunication technical deployment in developing countries'.
Ribauda B. 'When the walls have ears – business of technology- ambient intelligence technology', 2003.
Bohn, 2003
Cavoukian, 2004.
Data protection
SWAMI State of the Art Deliverable, Legal Part VUB.
Proportionality of data collection?
Sustainability of purpose specification by AmI Service providers?
Consent through intelligent agents?

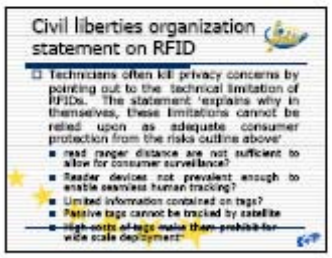
25

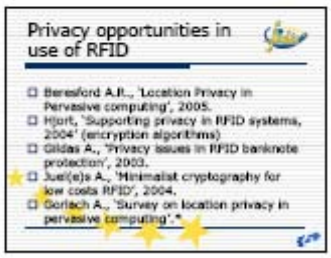

RFID privacy related problems
Garfinkel S., 'An RFID Bill of Rights', 2002
Gildas A., 'Privacy issues in RFID banknote protection', 2003.
Lewis 'RFID; small package, big problem', 2003.
Canoukhan A., 'Tag, you're it: privacy implications of Radio Frequency (RFID)', 2004.
Natsui T., 'Smart ID and Privacy in Japan. Legal issues of tracking using radio frequency identification (electronic tags)', 2003
Natsui T., 'Traceability System using RFID and Legal issues', 2004.


More on legal perspectives
Dumortier J., A decade of research @the crossroads of law and ICT, 2001.
Froomkin A.R., Legal issues in anonymity and pseudonymity. Information society, 1999
Hustinx 'EU/US Privacy self regulation, a decade of disappointment', 2003.
Lloyd regula G., 'Regulation of electronic employee monitoring - data privacy legislation in the EU, US and Canada', 2004.
De Hert P., 'Biometrics, legal issues and implications', 2005.
Ihde R., 'A face value. On biometric identification and privacy', 1999


7. Techical perspectives
Riva, Chapter 4, p 17. : International Organization for Standardization's ISO 13407 "Human centered design for interactive systems".
But "To the extent that security has been considered, it has mainly been an issue of network security rather than individual security." [first deliverable swami: 31 referring to Marc Langheinrich, (ETHZ), DC initiative called Troubadour.]

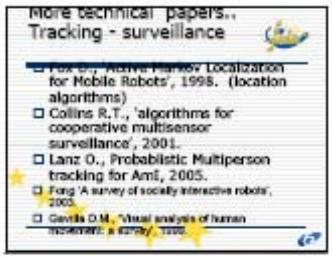

... - tags – chips – dust ...
•Raskar R., 'RFID tagging the world – photosensing wireless tags for geometric procedures', 2005.
•Yang S., 'Researchers create wireless sensor chip the size of glitter', 2003
•Smart Dust Project


Civil liberties organization statement on RFID
Technicians often kill privacy concerns by pointing out to the technical limitation of RFIDs. The statement 'explains why in themselves, these limitations cannot be relied upon as adequate consumer protection from the risks outline above'
read ranger distance are not sufficient to allow for consumer surveillance?
Reader devices not prevalent enough to enable seamless human tracking?
Limited information contained on tags?
Passive tags cannot be tracked by satellite
High costs of tags make them prohibit for wide scale deployment?


Privacy opportunities in use of RFID
Beresford A.R., 'Location Privacy in Pervasive computing', 2005.
Hjort, 'Supporting privacy in RFID systems, 2004' (encryption algorithms)
Gildas A., 'Privacy issues in RFID banknote protection', 2003.
Juel(e)s A., 'Minimalist cryptography for low costs RFID', 2004.
Gorlach A., 'Survey on location privacy in pervasive computing',".

26


Other user centric opportunities in Technical applications
Fine h., 'Informed intelligent environments: creating the profiled user interface', 2004.
Fuentes L., 'Towards the development of Ambient Intelligent Environments using Aspect-Oriented techniques', 2004.
Göker A., 'An Ambient Personalised and context sensitive information system for mobile users', 2004
Grill T., 'Agents for Ambient Intelligence – support or nuisance', 2004.
Jøsang A., 'Trust requirements in identity Management', 2005*.


More technical papers..
Tracking - surveillance
for Mobile Robots', 1998. (location algorithms)
Collins R.T., 'algorithms for cooperative multisensor surveillance', 2001.
Lanz O., Probabilistic Multiperson tracking for AmI, 2005.
Fong 'A survey of socially interactive robots', 2003.

27