



# Safeguards in a World of Ambient Intelligence (SWAMI)

## Final Report

### Deliverable D4

30 August 2006

*Editor*: David Wright

*Authors*: Pasi Ahonen, Petteri Alahuhta, Barbara Daskala, Paul De Hert, Sabine Delaitre, Michael Friedewald, Serge Gutwirth, Ralf Lindner, Ioannis Maghiros, Anna Moscibroda, Yves Punie, Wim Schreurs, Michiel Verlinden, Elena Vildjiounaite, David Wright

DRAFT – Subject of approval by the European Commission

**Project Co-ordinator:** Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research, Breslauer Straße, 76139 Karlsruhe, Germany, E-Mail: m.friedewald @ isi.fraunhofer.de

**Partners:**

Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany. Contact: Michael Friedewald. http://www.isi.fraunhofer.de

Technical Research Center of Finland, VTT Electronics, Oulu, Finland. Contact: Petteri Alahuhta (Petteri.Alahuhta @ vtt.fi). http://www.vtt.fi/ele/indexe.htm

European Commission/Joint Research Center-Institute for Prospective Technological Studies, Seville, Spain. Contact: Ioannis Maghiros (ioannis.maghiros @ cec.eu.int). http://www.jrc.es

Free University Brussel, Center for Law, Science, Technology and Society Studies, Belgium. Contact: Serge Gutwirth (serge.gutwirth @ vub.ac.be). http://www.vub.ac.be/LSTS/

Trilateral Research & Consulting, London, United Kingdom. Contact: David Wright (david.wright @ trilateralresearch.com). http://www.trilateralresearch.com/

**Project web site:** http://swami.jrc.es



We suggest the following citation format: Wright, David (ed.), *Safeguards in a World of Ambient Intelligence: Final Report*, SWAMI Deliverable D4: A report of the SWAMI consortium to the European Commission under contract 006507, August 2006. http://swami.jrc.es

**Contents**

# 1 EXECUTIVE SUMMARY

Ambient intelligence (AmI) holds considerable promise for Europe's economy and society. To be sure, there are technological and other challenges to be met in order to achieve all of the benefits promised by AmI, but the Commission, Member States, industry, academia and other stakeholders are rising to these challenges. Hundreds of millions of euros have already been spent in AmI research, and undoubtedly such high spend levels will continue.

While engineers and scientists have been focusing on the complexities of creating interoperable networks capable of supporting a wide variety of heterogenous devices, including those embedded in products, with widely differing capabilities, some scavenging energy from ambient sources, some self-configuring, some self-healing, some with a multitude of capabilities operating at broadband speeds, other researchers have been worrying about the implications AmI has for privacy, identity, trust, security and the digital divide.

The SWAMI project, funded under the EC's Sixth Framework Programme, was created to examine these issues. SWAMI is the acronym for Safeguards in a World of Ambient Intelligence, which perfectly describes what the project was all about.

At the outset of the project, in February 2005, the SWAMI partners began by reviewing well over 100 AmI-related projects in Europe, the United States and Japan to see to what extent the key issues of privacy, identity, trust, security and digital divide had been considered. Few projects had these issues as their prime focus, although more than a few did flag these issues.

We also looked at existing scenarios and analysed them with a view to understanding their implications in terms of these key issues. While most existing scenarios were describing the brave new world of AmI, how great it will be living and working in an AmI-enabled future, we often found that the technological marvels had some negative aspects that usually had not even appeared on the radar screens of the enthusiasts or, a less charitable view, perhaps some in industry have wanted to keep these negative aspects of the radar screens. Our first report also considered to what extent AmI and the issues it raised were adequately addressable by the existing legal frameworks. Or, to put it another way, were there some lacunae in the existing legal framework (which was not, after all, constructed with AmI in mind) if that framework was to address some of the issues raised in an AmI world? Our suspicions on that score proved well founded.

The first SWAMI report (*The brave new world of ambient intelligence*) had been submitted to the Commission by the time of our first expert workshop on 1 June 2005. We presented our key findings to the experts (of which there were 25, including the SWAMI partners). The workshop also had a focus on threats and vulnerabilities posed by AmI. The very good discussions at that workshop proved to be useful grist for an internal workshop held a month later where the partners brainstormed on scenario possibilities that would form the core of the second SWAMI report. As a result of that meeting, we agreed on and constructed four "dark scenarios", as we called them, a term coined to signify things that could go wrong in an AmI world, which were designed to expose some of the threats and vulnerabilities in AmI in the context of our key issues (privacy, identity, trust, security, digital divide).

The second report (*Dark scenarios in a world of ambient intelligence*) is noteworthy (in our perhaps not-so-humble opinion), not only because of the scenarios, but also the methodological structure we devised for both constructing and deconstructing scenarios, not just the SWAMI scenarios, but many other technology oriented scenarios. Our structured approach consists of a brief introduction, the scenario, a description of the scenario situation (its purpose, a very brief resume), the technologies referenced in the scenario, the applications, the drivers (what factors impel the scenario), the issues raised, including a legal analysis of the issues, and our conclusions.

Also, to ground our scenarios in reality – to ensure that they were not too far-fetched – we cited a good number of press reports in footnotes where somewhat similar situations have already begun to arise.

In addition to our scenario analysis *structure*, we think the *process* we followed to construct the scenarios was sound. The process is depicted below. Essentially, as shown in the figure, the partners made an extensive review of existing AmI-related projects and

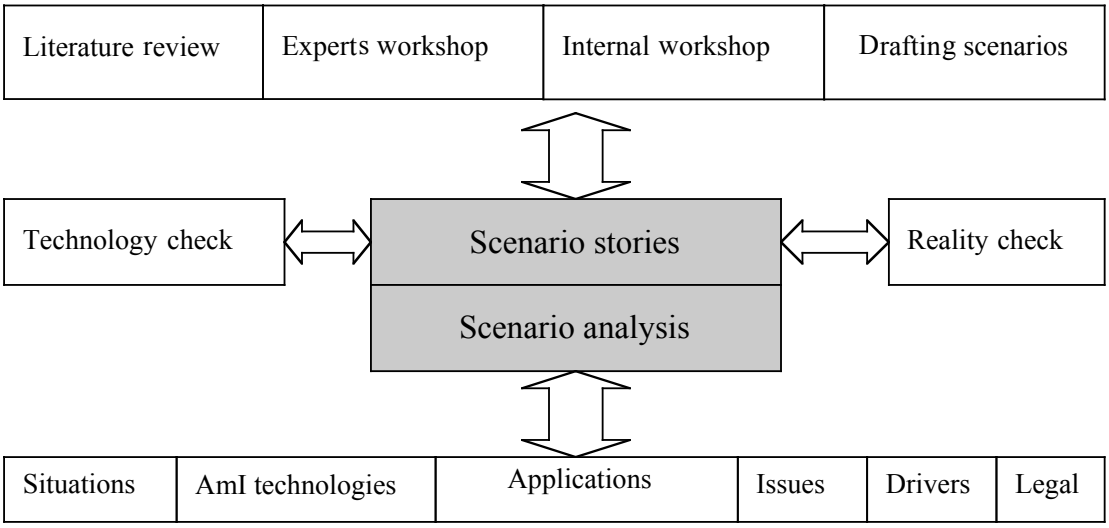


*Figure 1*

studies, with particular reference to the scenarios. We used the experts workshop to discuss the most important threats and vulnerabilities posed by AmI. We had our own internal workshop of SWAMI partners only where we brainstormed until we agreed the rough outlines of four contrasting scenarios. The partners then developed these outlines into scenario stories or scripts, and did a "technology check" (are the technologies referenced in the scenarios probable?) and a "reality check" (are there press reports of events similar to those mentioned in the scenarios?). Then all of the partners reviewed all of the scenarios in order to eliminate doubtful points, unnecessary wordage, irrelevancies, etc and to sharpen them to illustrate the points we wanted to emphasise. Once the scenarios were "stable", we performed our analysis of them (following the structured approach as described above), the last part of which was the legal analysis, which was able to consider not only the scenarios but also the analyses.

In addition to submitting our scenarios and analyses to the Commission in the second SWAMI report, we presented the scenarios at the second SWAMI expert workshop, held

in Brussels, 29 November 2005, and benefited from the comments of the experts too (including the SWAMI partners, 25 experts participated in the second workshop).

The second workshop was devoted to considering the main threats and vulnerabilities posed by AmI and, more especially, the safeguards that could help to minimise those threats and vulnerabilities.

From there, the partners went on to produce the third SWAMI report, entitled *Threats, vulnerabilities and safeguards in a world of ambient intelligence*. The partners produced a 34-page preview[1] of the third report, which was used as a kind of background paper or discussion paper for the final SWAMI conference, held in Brussels, 21-22 March 2006. More than 60 experts from Europe, the US and Japan attended the conference. Including representatives from the European Commission, there was a good mixture of experts and speakers from government, agencies, industry and academia. Based on the comments made at and after the conference, we judged the conference to have been highly successful. It focused on the same preoccupations as our third report. It was a good opportunity to exchange views, to hear presentations and benefit from discussions not only involving the SWAMI partners, but experts from outside the project, who had somewhat similar concerns as the SWAMI partners. To make sure we (and others) did not get too carried away in dwelling on the threats and vulnerabilities, we had a very polished presentation by Emile Aarts, who might be regarded as the "father of European AmI" (who coined the term ambient intelligence), to remind us and stimulate us with his vision of the benefits of AmI in many sectors and domains.

The SWAMI partners produced a 108-page summary report of the conference, which is available on the SWAMI website (http://swami.jrc.es) together with all of the presentations made at the conference.

The third SWAMI report discussed the issues of privacy, identity, trust, security and the digital divide, which was followed by a chapter on threats and vulnerabilities and a chapter on safeguards, before arriving at a final chapter containing our recommendations and conclusions, which were specifically addressed to the European Commission, Member States, industry, academia, civil society organisations and individuals. The third report contains many recommendations, some of which are technological, others socio-economic and still others which are legal and regulatory. While we would like to see all of the recommendations accepted and adopted by stakeholders, we had so many that we decided to create a "top six", i.e., those recommendations which we deemed most important. These are as follows:

1. The Commission, together with Member States, perhaps under the auspices of ENISA, should initiate a formalised risk assessment / risk management process with regard to the risks posed by AmI to security and privacy. We recommend that the assessment and decision-making process be open, transparent and inclusive, that stakeholder groups be identified and contacted and encouraged to take part in the process. Individuals should also be given an opportunity to express their views. Such a process could be initiated by means of a green paper on the risks to security and privacy in an AmI world. Whatever the outcome of the process, we recommend that the risk assessment be undertaken again (and

[1] The preview was entitled "Safeguards in a World of Ambient Intelligence (SWAMI): Policy Options to Counteract Threats and Vulnerabilities – First Results", Report submitted to the participants of the SWAMI conference, Brussels, 21-22 March 2006. http://swami.jrc.es.

again) in the future with some regularity, the periodicity of which might depend on the rapidity with which AmI is deployed (bearing in mind that the technologies for AmI are already being developed and deployed).

We also recommend that the precautionary approach be taken into account when developing and deploying new technologies. Such an exercise might be considered as a legal obligation.

2. The Commission and Member States should invest in an awareness campaign specifically focused on AmI, the purpose of which would be to explain to all stakeholders, but especially the public that AmI is on its way, that it offers great benefits, but also poses certain security and privacy issues. There are many ways of raising awareness (through education, the media, etc), but to give this recommendation some specific focus, we recommend that Member States hold annual national contests which would offer some form of recognition to the best product or service offering privacy and security protection. We recommend a run-off at European level. This could be a counterpoint to the notoriously bad publicity that ambient intelligence (especially RFID applications) has received in recent years.[2]

Any such campaign targeted at informing the public about ambient intelligence services and to inspire trust should involve *all* stakeholders, and any such competition should be judged by independent evaluators.

3. The Commission and Member States should review carefully the third SWAMI report and address the inadequacies and lacunae in the existing legal and regulatory framework with respect to AmI. Law is only one of the available tools for regulating behaviour, in addition to social norms, market rules and the "code", i.e., the architecture of the technology (e.g. cyberspace, ambient intelligence, mobile telephony…). The law can be a regulator on its own, but it can also regulate via influencing the "code" and other modalities of regulation.

The SWAMI consortium strongly recommends respecting this pluralism of modalities of regulation. In order to tackle the identified problems effectively, it is necessary to consider different approaches simultaneously.

4. The SWAMI consortium recommends that most of the challenges of new AmI environments be met by legal instruments that do not prohibit new technological developments, but channel them (such as by data protection and security measures). Transparency should be the default position, although some prohibitions referring to the political balances, ethical reasons or core legal concepts should be also considered in policy discussion. Focusing on concrete technologies rather than trying to produce general solutions seem to be more appropriate for AmI, an environment that adapts and responds to the changes of context, and in which privacy and other legal issues are also context-dependent. Thus, in developing policy options, one should focus on the concrete technologies, and apply channelling and prohibitive approaches accordingly.

---

[2] RFID technologies and their promoters have received Big Brother Awards in various countries world-wide. See e.g. http://bigbrotherawards.de/2003/.cop/; http://www.edri.org/edrigram/number4.3/frenchbba?PHPSESSID=a08c4d85ac916daab3d8660a1d377dd8; http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-187899; http://www.bigbrotherawards.cz/en/winners_2005.html

5. The biggest weakness in enforcement of rights is the limitation of any European rule to Member States only, or to countries which have signed international conventions such as the Cybercrime Convention). Clearly, ICTs and AmI have global dimensions. International co-operation in developing and enforcing the legal framework is necessary. Therefore, the Commission and Member States should be proactive in the development of a more comprehensive international co-operation framework that would take AmI technologies and capabilities into account as a matter of urgency.

6. The European Commission should ensure that projects that it funds take questions of privacy, security and trust into account. Research programmes should contain a project line of accompanying measures covering the societal impact. Currently, EC calls say that project participants must conform to relevant EU legislation, inter alia, the data protection directive (95/46/EC). It is, of course, necessary that project participants (or any third party funded by the EC) conform to EU legislation, but we think the Commission should be more demanding – i.e., it should require those it funds to specifically speculate what privacy or security impacts might arise from their projects and what measures should be taken to address those. In other words, simply conforming to legislation is not enough. Project participants must be asked to foresee or even to speculate what privacy or security implications their projects *might* have. By the same token, the EC proposal and tender evaluators should also be asked to evaluate project proposals and tenders from the same optic. We recommend that Member States adopt a similar approach. We would like to especially emphasise the importance of funding research on technological safeguards for protecting privacy and enhancing security and for overcoming the digital divide. If technology does not provide solutions for human-technology interfaces for all, or for user-friendly security, other safeguards will not be able to solve the problem. We suggest that among technological safeguards research on intelligent algorithms is especially important.

SWAMI partners believe that, sooner or later, we will live in a world of ambient intelligence. For ambient intelligence to be a success story, in human terms, according to democratic principles, and not to be an Orwellian world, all stakeholders must be cognisant of the threats and vulnerabilities and work together to ensure adequate safeguards exist. Certainly, industry should become more active in creating applications that are secure and privacy enhancing since this is the major way to create consumer trust and make ambient intelligence fruitful to *all* participants. Industry should not view privacy, security, identity, trust, and inclusion issues as regulatory barriers to be overcome. Rather, they should regard such measures as necessary, justified and, in the end, crucial to ensuring that their fellow citizens will use ambient intelligence technologies and services. In the meantime, we encourage all stakeholders to be vigilant.

* * *

This fourth SWAMI report is essentially a summary of the first three reports. The reader interested in more details is encouraged to go to the original reports, notably the first three deliverables, which are entitled *The brave new world of ambient intelligence*, *The dark scenarios* and *Threats, vulnerabilities and safeguards in a world of ambient intelligence*, all of which can be found on the SWAMI website at http://swami.jrc.es.

# 2 INTRODUCTION

In the Technical Annex to the SWAMI contract, the partners committed themselves to production of a draft final report, incorporating the earlier reports produced in WPs 1, 2 and 3, as modified taking into account the comments gathered from the workshops and the customer. The report was to be – and is – in several parts, comprising a synthesis and overview of existing AmI scenarios, roadmaps, projects, studies and their salient points; the dark scenarios for ambient intelligence; identifying lacunae in existing policies and programs and the social and policy options for overcoming those lacunae; and the SWAMI project's conclusions and recommendations. In addition, the partners were to collaborate in the production of an executive summary (see above).

As this report is a synthesis, it does not pretend to be a comprehensive integration of our earlier reports. For example, in the review of other AmI-related projects, we provide a very few examples, rather than the much more exhaustive review contained in our first report. Similarly, we provide only one of the dark scenarios – as an example – rather than all four of those that we developed for our second report. Nor does this report present all of our review of the existing legal framework, nor all of the lacunae we have spotted, nor all of our considerations for adapting the legal framework in order to deal with an AmI-enabled future. Even though we have had to summarise much of what was contained in our earlier reports, this final report is still quite detailed and does give, we trust, a relatively rounded picture of our findings and thinking about the threats and vulnerabilities posed by AmI to the key issues of privacy, identity, trust, security and the digital divide as well as the safeguards that we think need to be put in place. As mentioned above, the reader interested in more detail and greater elaboration should refer to the earlier SWAMI reports on which this one is based.

# 3 OVERVIEW OF EXISTING AMI PROJECTS & STUDIES

Ambient intelligence presents a vision of the Information Society where the emphasis is on greater user friendliness, more efficient services support, user empowerment, and support for human interactions. People are surrounded by easy-to-use interfaces that are embedded in all kinds of objects and by an everyday environment that is capable of recognising and responding to individuals in a seamless, unobtrusive and invisible way.

The human factor is crucial in the construction of safeguards in a world of ambient intelligence. The success of ambient intelligence will depend on how secure its use can be made, how privacy and other rights of individuals can be protected and, ultimately, how individuals can come to trust the intelligent world which surrounds them and through which they move. The European Commission has acknowledged and emphasised this dependency between technology and trustworthiness on numerous occasions.[3]

There is a clear need to consider ambient intelligence technologies and developments in the context of how the rights of individuals can best be protected and to formulate adequate social and policy options. Such consideration will contribute to the European policy development. Indirectly, this can also contribute to the scientific and technical aspects in so far as it will highlight various options that should be taken on board by other projects of a more scientific and technical nature, that is, those who are involved in scientific and technical projects should be cognizant of their policy implications. It is already obvious that realising the vision of ambient intelligence will require more than just technology and, as has happened throughout history, especially in the last decade or so, significant technological advances almost always raise policy issues.

While the world of ambient intelligence will undoubtedly bring many benefits, trust and security should be designed into this world rather than inserted as an afterthought into an already constructed world of smart spaces. However, this goal is not possible to achieve in reality, at least not completely, in part because there are already islands of ambient intelligence and, in any event, the notion of "absolute security" is not feasible, as has been pointed by many experts, e.g., in the US Research Council report *Trust In Cyberspace*[4], and Bruce Schneier in his books *Secrets and Lies* and *Beyond Fear*. The nature of AmI networks, like existing networks such as the Internet, is such that they evolve, and new software and technologies are added by many different people and entities. Thus, building trust and security into networks inevitably involves an effort of trying to create trustworthy systems from untrustworthy components. The success of this brave new world will depend on its acceptability by citizens and by taking steps to minimise their concerns with regard to how it might lead to further encroachments upon their privacy, safety and security.

The European Commission has recognised these challenges. It has stated that "multidisciplinary research is needed on the social, legal, organisational and ethical issues

[3] Protection of privacy is a key policy objective in the European Union. It was recognised as a basic right under Article 8 of the European Convention on human rights. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union provide the right to respect for family and private life, home and communications and personal data. The Directive of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (2002/21/EC) has similar provisions.

[4] Schneider, F. B. (ed.), *Trust in Cyberspace*, National Academy Press, Washington, D.C., 1999.

associated with ambient intelligence, which places the individual at the centre of future developments for an inclusive knowledge based society for all. This includes also the investigation of the emerging challenges, in particular with respect to identity, privacy and protection of rights for all citizens in all their roles (private and professional) in the Information Society. It is important to identify new societal and policy options including responsibilities and ethics of digital behaviour. The task also requires research, on how to build into Information Society services and systems the safeguards and privacy enhancing mechanisms needed to ensure user control and enforceability of policy in an accessible manner."[5]

The SWAMI project (Safeguards in a World of Ambient Intelligence) aimed to address these issues. It had three major tasks:
1. To identify the social, legal, organisational and ethical implications related to issues such as privacy, anonymity, manipulation and control, and identity in the context of ambient intelligence using current and future information and communications technologies.
2. To create and analyse four "dark" scenarios on AmI that highlight and detail the key socio-economic, legal, technological and ethical risks related to, in particular, identity, privacy and security. The scenarios are called dark because they present visions of the future that we do NOT want to become realities. Their objective is to expose risks and vulnerabilities as a way to inform policy-makers and planners to be aware of the dangers of these possibilities.
3. To identify research and policy options on how to build into Information Society services and systems the safeguards and privacy enhancing mechanisms needed to ensure user control, user acceptance and enforceability of policy in an accessible manner, with a view to support accessibility and the provision of citizens with real equal rights and opportunities in a world of Ambient Intelligence.

This chapter provides an overview of ambient intelligence research in Europe, the United States and Japan, with a particular focus on the issues of privacy, identity, security, trust and the digital divide. In view of the significant amount of research, this chapter cannot be regarded as being a comprehensive survey by any stretch of the imagination. It does, however, highlight some of the most important visions, scenarios, research agendas, projects and platforms. For more detail, those interested may wish to check out Annex 1 of the first SWAMI report (*The brave new world of ambient intelligence*), which provides a longer list of projects and their associated websites.[6]

## 3.1 AMI RESEARCH IN EUROPE, THE UNITED STATES AND JAPAN

Ambient intelligence is expected to yield many benefits for European citizens and consumers, industry, commerce and the provision of public services. It has attracted a lot of interest in Europe from the European Commission, industry, universities, research institutes and other stakeholders. Hundreds of millions of euros have been spent and are

[5] European Commission, Work Programme for the specific programme for research, technological development and demonstration: "Integrating and strengthening the European Research Area": Specific activity covering policy-orientated research under 'Policy support and anticipating scientific and technological needs' (SSP Call 3), Brussels, 2003.
[6] See also Wright, David, "The dark side of ambient intelligence", *Info*, Vol 7 No. 6 [October 2005], pp 33-51. www.emeraldinsight.com/info

being spent on AmI projects. Realisation of the AmI vision, however, poses many challenges, many of which are technical, some of which are what might be described as organisational, and still others which involve societal issues.

While most stakeholders paint the promise of AmI in sunny colours, there is a dark side to AmI as well. In a way, this dark side is inherent in the very nature of AmI, i.e., the fact that AmI technologies will deliver personalised services to users means that a lot of personal information is stored somewhere with risks that the user's personal information can be abused, either accidentally or intentionally. These risks have been recognised by policy-makers and researchers, and are at the heart of the SWAMI project. In view of these risks, some AmI experts have been working on potential safeguards against such abuse.

Hence, one task before SWAMI was to review AmI projects and studies in Europe, the United States and Japan in order to determine to what extent the key issues of privacy, identity, security, trust and what is sometimes called the digital divide have been taken into consideration and to see, where that has been the case, what safeguards others have proposed. We looked at more than 70 AmI projects in Europe and a similar number in the United States and Japan. We also looked at various studies, reports and other documents. We structured our review of research in Europe, the US and Japan according to visions, scenarios, roadmaps, research agendas and projects, as each category is distinct and serves a different purpose, although one leads logically to the next.[7]

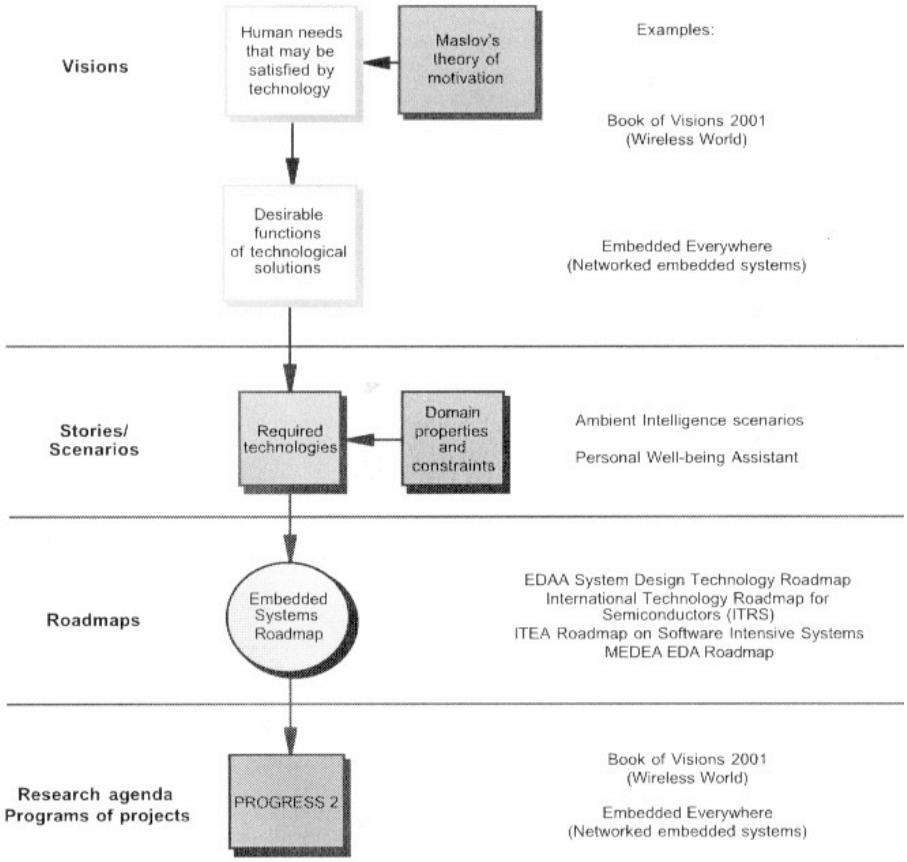


Figure 1: Positioning of the Embedded Systems Roadmap

[7] We adopted the schema of visions, scenarios, roadmaps, research agenda and projects from the diagram on p. 4 of the *Embedded Systems Roadmap*. See www.stw.nl/progress/ESroadmap/index.html

As one might expect, not all of these visions, scenarios, roadmaps, research agendas and projects have taken the above-referenced issues into account, although many have. We also considered the platforms, i.e., the way in which industry, governments and other stakeholders have organised themselves to undertake the shared research agendas.

## 3.2 AMBIENT INTELLIGENCE IN EUROPE

### 3.2.1 Visions

Many projects have visions of what they want to do or, more expansively, of the future world of ambient intelligence. However, most such visions are not elaborated to any great extent. Nevertheless, several important visions of AmI have been produced.

Perhaps the best-known vision document, the one most elaborated, is *The Book of Visions*, which provides a vision of our technological future, or at least our wireless technological future. It resulted from an initiative of several large European companies and Motorola who came together to form the Wireless World Research Forum (WWRF).[8] *The Book of Visions* includes ambient intelligence within its scope. The first version of the Book appeared in 2001.[9] The vision was of a future 10 –15 years away.

There is some interesting discussion in *The Book of Visions* about profiling users, especially in the context of personalisation of services, security and privacy. It observes that without access to user-related context data many mobile services would not exist and that the issue of incomplete context-information (or profile data) must be solved.[10] In the envisaged security and privacy layer of future networks, customers should have the means to decide their security policies in a simple way.

Gathering profile data and keeping it up-to-date is regarded as an important issue. Thus, future networks should be embedded with a "profile learning functionality".[11]

While some of the statements in *The Book of Visions* might serve only to heighten anxieties about privacy risks, nevertheless, the WWRF has established a Special Interest Group (SIG 2) which is addressing threats to privacy and security and what industry should do about them.

Another similarly well-known AmI vision is that produced by the Information Society Technology Advisory Group (ISTAG), which advises the European Commission's

[8] www.wireless-world-research.org. Strictly speaking the WWRF is not a European organisation, but in view of the prominence of European companies, and the utility of its Book of Visions, it is referenced in this chapter nevertheless. See the section on platforms for more about the WWRF.
[9] www.wireless-world-research.org/general_info/BoV2001-final.pdf. The most recent version of the Book of Visions was published in April 2006 by Wiley. http://www.wireless-world-research.org/general_information/book_of_visions.php
[10] WWRF, *The Book of Visions 2001: Visions of the Wireless World*. Version 1.0. Wireless World Research Forum, 2001, p.39. http://www.wireless-world-research.org/general_info/BoV2001-final.pdf.
[11] WWRF, The Book of Visions 2001, p 128.

Information Society Directorate General. In September 2003, ISTAG published a report called *Ambient Intelligence: from vision to reality*.[12]
ISTAG sees "significant opportunities" for AmI in relation to:

- modernising the European social model particularly in terms of: improving civil security; providing new leisure, learning and work opportunities within the networked home; facilitating community building and new social groupings; providing new forms of healthcare and social support; tackling environmental threats; supporting the democratic process and the delivery of public services.
- improving Europe's economy in terms of: supporting new business processes; increasing the opportunities for tele-working in the networked home; enhancing mobility and improving all forms of transport; supporting new approaches to sustainable development.[13]

While ISTAG has a generally sunny outlook with regard to AmI, it does see at least one dark patch. It says the anticipated benefits of ambient intelligence may be numerous but the enabling technologies can also facilitate monitoring, surveillance, data searches and mining, as a result of which AmI deployment is likely to be of great concern to citizens, civil liberties groups, governments and industry. Addressing the balance between privacy and security will, it says, be a core challenge for the future. [14]

### 3.2.2 Scenarios

From visions, one can build scenarios. Building scenarios is a useful tool for the development and application of new technology. Scenarios could be seen as closely related to storytelling, as they are a way of projecting new situations showing the application and/or consequences of new technologies. Scenarios anchor the design process and, at the same time, are intended to provoke reflection on situations of use, both as they occur in the real world and in the future.[15]

Scenarios are not traditional extrapolations from the present, but offer provocative glimpses of futures that can (but need not) be realised. Scenario planning provides a structured way to get an impression of the future and to uncover the specific steps and challenges in technology that have to be taken into account when anticipating the future. To put it another way, scenario planning is a tool to help us invent our future.[16]

Most scenarios show the benefits of AmI or deal with specific issues, but a few considered "dark" scenarios (to use a SWAMI terminology). Often what makes a scenario "dark" are deficiencies with regard to privacy, security, identity and other issues of direct concern to SWAMI.

---

[12] IST Advisory Group, *Ambient Intelligence: From Vision to Reality*. For participation – in society and business, Office for Official Publications of the European Communities, Luxembourg, 2003. http://www.cordis.lu/ist/istag-reports.html
[13] ISTAG 2003, p. 9.
[14] ISTAG 2003, pp. 11 et seq.
[15] Welen, P., A. Wilson and P. Nixon, *Scenario Analysis*, Gloss Deliverable D.9, University of Strathclyde, Glasgow, 2003, p. 6. http://iihm.imag.fr/projects/Gloss/Deliverables/D9-1.pdf.
[16] IST Advisory Group, K. Ducatel, M. Bogdanowicz et al., *Scenarios for Ambient Intelligence in 2010*, EUR 19763 EN, EC-JRC, Institute for Prospective Technological Studies (IPTS), Sevilla, 2001, p. 1. http://www.cordis.lu/ist/istag-reports.html.

In this context, it is useful to consider the RAPID roadmap project which introduced three scenarios for the uptake of privacy and identity management (PIM) in society:

- In the first (positive) scenario, identity management integrated with privacy protection adds value for users, business and government.
- In the second ("steady state") scenario, identity management and privacy protection are two different worlds. Privacy protection is for special niche markets with a strong battle between law enforcement and privacy protection. In this scenario, PIM grows slowly in special markets and delivers only a baseline protection.
- In the third (negative) scenario, users are not interested in identity management and privacy protection. Users expect active use of their profiles by business and government for value added and cheaper services. PIM is less important, PIM regulation will be stripped, users lose interest in privacy, and PET companies go bankrupt.

### 3.2.3 Roadmaps to the future

Roadmaps follow on from scenarios – i.e., to realise a scenario, roadmaps set out what steps must be taken. Roadmaps provide an overview of technology development by mapping out gaps, barriers and bottlenecks to be overcome.

Roadmaps were developed during the 1980s as a strategic planning tool by (mainly American) corporations and use of the tool was later extended for the purposes of entire industry sectors. In recent years, roadmapping has also been applied to an increasingly broad range of areas such as trans-disciplinary high-tech common goals or the provision of intelligence for S&T policy-making.[17]

There are several European AmI-relevant roadmaps. One of the first was the *PROGRESS Embedded Systems Roadmap 2002*[18] produced by the Dutch embedded systems community at the behest of the Technology Foundation STW, the Dutch funding agency for university research. The roadmap was published in 2002.

The RAPID project (July 2002-June 2003)[19] developed a strategic roadmap for applied research in the area of privacy and identity management. The project built a platform of and forum for experts and stakeholders from industry, academic and research institutions and civil rights organisations, and covered the domains of privacy enhancing technologies, IT security, law and IT, and socio-economic issues.

### 3.2.4 Strategic research agendas

From roadmaps, research agendas can be developed which indicate what areas must be researched in order to bring visions into reality. Quite a few European projects have developed research agendas important to AmI. Among those are the following:

[17] Da Costa, O., M. Boden, Y. Punie, M. Zappacosta, "Science and Technology Roadmapping from Industry to Public Policy", in *The IPTS Report* 73, 2003, pp. 27-32.
[18] PROGRESS is the acronym for PROGram for Research in Embedded Systems and Software. The roadmap can be found at www.stw.nl/progress/ESroadmap/index.html
[19] RAPID is the acronym for Roadmap for Advanced Research in Privacy and Identity Management. The project had a budget of €399,134 and eight partners.

The eMobility platform has also published a strategic research agenda, available on its website.[20] Major sections of its research agenda deal with ambient services, ambient connectivity, and security and trust.

The ARTEMIS platform has also developed a strategic research agenda, which, inter alia, addresses research as well as infrastructural issues, including co-ordination with Eureka's ITEA and MEDEA+ programmes.

### 3.2.5 Platforms

There are many players in AmI development in Europe. To harness their efforts and ensure congruence, some organisational arrangements must be put in place. That is essentially the function of a platform. Technology platforms bring together companies, research institutions, financial institutions and regulatory authorities to define a common research agenda and to mobilise the necessary resources for implementing that agenda.[21] In some sense, this is also what the EC-funded Networks of Excellence and Integrated Projects do.

The Commission began promoting European technology platforms in 2003 and encouraged interested parties to come together and set up platforms at European level. The European Commission continues to emphasise the importance of platforms as vehicles for public-private partnerships in stimulating competitive research while ensuring the complementarity of action at national, trans-national and European level.[22] Platforms are also regarded as an important instrument in tackling the relaunched objectives of the Lisbon Council. The Commission has taken the platforms' research agendas into account in framing the Seventh Framework Programme (FP7) and, in line with that, foresees joint technology initiatives as a way of implementing them and as a new instrument in FP7. It also is considering appropriate legal structures. The Commission has a website (www.cordis.lu/technology-platforms/summaries.htm) devoted to platforms across many research areas and of those, two relate to AmI, namely those of ARTEMIS (embedded systems) and eMobility (mobile and wireless communications technology):

*Wireless World Research Forum (WWRF)*

The Wireless World Research Forum (WWRF), founded in 2001 by Alcatel, Ericsson, Motorola, Nokia and Siemens, is open to all interested parties and includes manufacturers, network operators and service providers, R&D centres, universities, and small and medium enterprises (SMEs). As mentioned above, the WWRF produced *The Book of Visions*. The WWRF has six working groups and several special interest groups, one of which (SIG2) deals with security and trust issues. SIG 2 aims to identify and promote research areas that

[20] www.emobility.eu.org

[21] European Commission, *Technology Platforms: from Definition to Implementation of a Common Research Agenda*: Report compiled by a Commission Inter-Service Group on Technology Platforms, Office for Official Publications of the European Communities, Luxembourg, 2004. http://www.eurogif.org/wimages/Technology_Platforms_21_September_2004.pdf

[22] See European Commission, *Science and technology, the key to Europe's future - Guidelines for future European Union policy to support research*, COM(2004) 353 final, Brussels, 2004. ftp://ftp.cordis.lu/pub/era/docs/com2004_353_en.pdf and European Commission, *Report on European Technology Platforms and Joint Technology Initiatives*: Fostering Public-Private R&D Partnerships to Boost Europe's Industrial Competitiveness, Commission Staff Working Document, SEC(2005) 800, Brussels, 2005.

might resolve the needs of users, operators, service providers and other players for secure and trustworthy wireless systems.

*ARTEMIS*

ARTEMIS[23] is a sort of public-private partnership which aims to mobilise and co-ordinate private and public resources to meet business, technical and structural challenges in embedded systems and to ensure that systems developed by different vendors can communicate and work with each other via industry standards. The organisational structure, extent of industry involvement, support from the Commission, all indicate that ARTEMIS is likely to be the European body with an overarching view and remit dealing with embedded systems (ambient intelligence).

Although it has already established several working groups, none of them deals with privacy, security, identity, digital divide and other such issues. Although the *Building ARTEMIS* report only uses the word privacy twice, nevertheless, with regard to security, it recognises that it is of the utmost importance to avoid any compromises to security in embedded systems and that systems must conform to legal frameworks with regard to security, trust, contracts and liability. It says that embedded systems must be robust to usage and resistant to malicious attack and fraud.

*eMobility*

eMobility is a mobile and wireless communications technology platform, established by industry and operators in 2004. Its objective is to reinforce Europe's leadership in mobile and wireless communications and services and to master the future development of this technology. It says security and trust must feature in future business models and that commercial success depends on user confidence. The security framework of the future should contain evolved security mechanisms in the areas of authentication, encryption, identity management, privacy, digital rights management, and trusted transactions environment.

### 3.2.6 Projects

Of the more than 70 European projects reviewed by SWAMI, about a fifth are devoted to privacy, identity and (personal) security issues or treat these issues in a substantive way. The four biggest projects (PISA, PRIME, FIDIS and GUIDE) had or have substantial budgets, ranging from €3.2 million and nine partners (PISA) to €13.14 million and 21 partners (PRIME). The privacy projects mainly focused on privacy enhancing technologies and identity management in the context of legal requirements.

## 3.3 Ubiquitous computing in the United States

There has been and continues to be a huge amount of research on ubiquitous computing in the US, far beyond that in other non-European countries. As with Europe, the SWAMI

[23] ARTEMIS is the acronym for Advanced Research and Development on Embedded Intelligent Systems. The same acronym was also used in a Dutch-sponsored AmI project called ARTEMIS: ARchitectures and meThods for Embedded MedIa Systems. The latter project finished in June 2004. See the website www.onderzoekinformatie.nl/en/oi/nod/onderzoek/OND1277482/

team reviewed US projects and studies to understand what work has been done or is being done on safeguards for privacy, identity, individual security and so forth as well as to consider what measures, if any, are being taken to avoid a digital divide.

A review of ubiquitous computing research in the United States needs to be seen against the backdrop of security, especially since 11 September 2001. Security was already an issue before then, but has been greatly magnified since. Security can be considered in the context of computer communications networks and systems and the infrastructures they support as well as in the context of or from the perspective of individuals.

Much of the research on ubiquitous computing has been undertaken in the universities, such as the University of California at Berkeley, Stanford, Cornell, Carnegie Mellon, Yale, Harvard, etc. They have been heavily supported by government funding. The largest pool of funding for research is that of the Defense Advanced Research Projects Agency (DARPA)[24], which is the central research and development organisation for the Department of Defense (DoD). Probably the next most important source of funding for cyber security research is the National Science Foundation (NSF)[25], an independent federal agency with an annual budget of about $5.5 billion. The Department of Homeland Security (DHS) is growing in importance as a source of funding for cyber security research.[26] Government agencies such as the Energy and Transportation departments have been funding ubiquitous computing research as well.

Many large companies have been undertaking ubiquitous computing research, either on their own or in consortia with other companies and/or universities. Among the companies are Microsoft, IBM, Xerox, HP, Intel, Motorola, Cisco Systems, Sun Microsystems, etc. We have not made a determination of the overall funding by the corporate sector of research on ubiquitous computing, but to give one indicative example, IBM has said it plans to spend $250 million during the next five years on embedded technology and has created a "sensors and actuators" unit to that end.[27]

### 3.3.1 Visions

It's been said that the *Embedded Everywhere* report published by the National Academy of Sciences (NAS) is a vision document, but in fact it is explicitly a research agenda.[28] Nevertheless, as its title suggests, it does contain some visions of the future. For example, with networking sensors embedded everywhere, it foresees the day when we will have an Internet of things.[29]

---

[24] www.darpa.mil

[25] www.nsf.gov/index.jsp

[26] The Homeland Security Advanced Research Projects Agency (HSARPA) will spend about $390 million in its current fiscal year with small and large companies to develop a range of next-generation technologies. Areas of focus will include networked biological and chemical sensors; systems architectures for managing sensor networks; radiation and nuclear-threat detection systems, as well as decontamination systems; 'over-the-horizon' sensors for ships; and other programs still in development (Merritt 2004).

[27] IBM predicts wireless sensor nets could represent a $6 billion overall market by 2007, with the bulk of profits from software that helps the devices better communicate and lets customers interpret data from them (Ricadela 2005).

[28] Estrin, Deborah (ed.), *Embedded, Everywhere*: A Research Agenda for Networked Systems of Embedded Computers, National Academy Press, Washington, D.C., 2001.

[29] The phrase "Internet of things" comes from an article with the same title by Chana R. Schoenberger in *Forbes* magazine, 18 March 2002. The author quotes Kevin Ashton, an executive at Procter & Gamble who

The authors of the *Embedded Everywhere* opined that "Privacy may be at much greater risk than at any previous time in history." Alarming, at least for some, many people don't seem that bothered. They are quite willing, especially post 11 September, to forego some of their right to privacy in exchange for better security. However, some of the same profiling and data mining technologies which can be used to improve security can also be used for surveillance and to bombard people with unwanted advertising. Accordingly, the erosion of personal privacy, identity theft and other downsides of the brave new world we live in have inspired some ubiquitous computing projects and studies in the United States, just as they have in Europe.

### 3.3.2 Scenarios

Based on our research so far, there seems to be fewer exercises in drawing scenarios, dark or otherwise, in the United States compared to Europe. Those scenarios that do exist in the ubiquitous computing domain are rather more functional than those in Europe. In the *Embedded Everywhere* report, there are three scenarios relating to the use of Emnets (as they are called) in the automotive, agricultural and defence sectors. They don't map out alternative futures, so much as show how the new technologies can be used. In fact, those scenarios are firmly grounded in today's technologies. They merely extend what's available today to what's likely to be available tomorrow.

A few of the projects reviewed for this chapter do carry scenarios akin to those of the ISTAG studies among others in Europe. The Oxygen project at MIT is one such example. The AURA project at Carnegie Mellon University also uses scenarios.[30] Another is the Portolano project which comes not only with a "screenplay" and analysis, but even with cartoons.[31]

The *Who Goes There?* report has two very good scenarios to illustrate the ways in which identification and authentication arise in everyday life and to highlight some of the important issues associated with new systems.[32] The first scenario describes the life of Joseph K as he goes on a business trip. The second describes a token-based authentication system used by Laura on a visit to a hospital.

### 3.3.3 Roadmaps

Though roadmapping was developed in the US as a strategic planning tool for industry in outlining how we should get from here to there, from today to tomorrow, fewer instances of broader, more policy-oriented roadmapping in the US than in Europe have become evident from our research.

---

heads the Auto ID Center at MIT: "We need an internet for things, a standardized way for computers to understand the real world." www.forbes.com/global/2002/0318/092.html

[30] Garlan, D., D. Siewiorek, A. Smailagic and P. Steenkiste, "Project Aura: Toward Distraction-Free Pervasive Computing" in *IEEE Pervasive Computing* 21, No. 2, 2002, pp. 22-31.

[31] http://portolano.cs.washington.edu/scenario/

[32] Kent, S. T. and L.I. Millett, (eds.), *Who Goes There? Authentication Through the Lens of Privacy*. National Academies Press, Washington, DC, 2003, pp. 21-27.

The best known roadmap, at least in the world of semiconductors, is the International Technology Roadmap for Semiconductors (ITRS),[33] which is an assessment of the technological challenges and needs facing the semiconductor industry 15 years into the future and potential solutions. The ITRS roadmap is, however, a technical document and does not deal with the "softer" issues of privacy, identity, security or even applications of semiconductors.

### 3.3.4 Research agendas

The National Academy of Sciences (NAS) has published several important reports which have served as research agendas for embedded systems and ubiquitous computing. Among them are the *Embedded Everywhere* report (published in 2001), which is undoubtedly the best known, *Who goes there? Authentication through the lens of privacy* (2003), *Trust in Cyberspace* (1999), and, most recently, a summary report from a workshop on *Radio Frequency Identification Technologies* (2004).

Although the *Embedded Everywhere* report was published in 2001, it has lost none of its validity and continues to reward those who go through it. The report discusses five features that must, it says, be addressed from the outset in the design of networked systems of embedded computers (abbreviated to EmNets, a term used throughout the report): reliability, safety, security, privacy, and usability, which can be encapsulated in the term "trustworthiness".

The report says that an issue that will need to be resolved is how (and sometimes whether) to advise people when their actions are being monitored. When should notification be mandatory? How can users be effectively signalled? Given individual differences in sensitivity and awareness, it may be difficult to provide adequate notification to some without annoying others.[34]

It says a fundamental issue is the ability of individuals to control the collection and dissemination of information about them in an environment in which daily transactions and events – and the events associated with their personal environment – involve EmNets or are controlled or monitored by them … privacy issues cannot be addressed by education and personal policies alone. Rather, they become (even more) a matter of public policy.[35]

The *Who goes there?* report examines the potential privacy impact of authentication technologies on four areas of privacy, each of which has a constitutional basis in the United States:
1. Bodily integrity, which protects the individual from intrusive searches and seizures;
2. Decisional privacy, which protects the individual from interference with decisions about self and family;
3. Information privacy, which protects the individual's interest in controlling the flow of information about the self to others; and

[33] http://public.itrs.net/
[34] Estrin, Deborah (ed.), *Embedded, Everywhere*: A Research Agenda for Networked Systems of Embedded Computers, National Research Council, National Academy of Sciences, National Academy Press, Washington, D.C., 2001, pp. 135 et seq.
[35] Estrin, p. 137.

4. Communications privacy, a subset of information privacy that protects the confidentiality of individuals' communications.[36]

The report identifies four overarching privacy concerns that broadly characterise the risks to personal privacy that authentication systems can create:
*Covert identification*. Some authentication systems make it possible to identify an individual without the individual's consent or even knowledge. Such systems deny the individual, and society, the opportunity to object to and to monitor the identification process. These technologies are particularly vulnerable to misuse because their use is hidden.
*Excessive use of authentication technology*. Led by a mentality of "more is better," the public and private sectors have been quick to increase the collection of personal information where this process is supported by cheaper, easier technology.
*Excessive aggregation of personal information*. The use of a single identifier (such as the Social Security number) or a small number of identifiers creates the opportunity for more linking of previously separate repositories of personal information.
*Chilling effects*. Wherever identity authentication is required, there is an opportunity for social control. [37]

### 3.3.5 Platforms and organisations

In Europe, platforms are rather specifically defined and there are some good examples of platforms, bringing together industry, government, research institutes, funding bodies, regulators, etc, to tackle the elaboration and implementation of a particular research agenda. There are not so many good examples in the United States. Thus, for the purpose of this section, the term has been used more broadly to identify associations, alliances and lobby groups that are focussed on ubiquitous computing and/or privacy enhancing measures.

Among the noteworthy platforms (=alliances, associations, lobby groups) that are somewhat focused on ubiquitous computing and/or privacy and related issues are the following:

*ZigBee Alliance*

The ZigBee Alliance[38] is a California-based association of companies working together to enable wirelessly networked, monitoring and control products (like smart dust) based on an open standard.

*Platform for Privacy Preferences Project (P3P)*

The Platform for Privacy Preferences is a set of standards that allow organisations to declare their privacy policies. The Platform for Privacy Preferences Project (P3P),[39] developed by the World Wide Web Consortium, is emerging as an industry standard

[36] Kent, Stephen T., and Lynette I. Millett (eds.), *Who Goes There?: Authentication Through the Lens of Privacy*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academies Press, Washington, DC, 2003, p. 63.
[37] Kent and Millett, pp. 30f.
[38] www.zigbee.org
[39] www.w3.org/P3P/#what

providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit.

*Liberty Alliance*

The Liberty Alliance[40] with a membership of more than 150 companies, non-profit and government organisations has developed an open standard for federated network identity which, it says, offers businesses, governments, employees and consumers a convenient and secure way to control identity information.

*TRUSTe*

TRUSTe[41] is an independent, non-profit organisation founded in 1997 by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium with sponsors including AOL, Intuit, Japan Engineers Foundation and Microsoft. TRUSTe awards a trustmark, which signifies that TRUSTe recognises companies that are doing the right thing in online privacy. TRUSTe says it maintains the largest privacy seal programme with more than 1,400 Web sites certified throughout the world.

*EPIC*

The Electronic Privacy Information Center (EPIC) is a public interest research centre in Washington, D.C., focusing on civil liberties issues and privacy. EPIC is working with other privacy organisations to prevent abuse of RFID technology. EPIC also objects to the government's extensive support for surveillance research.

### 3.3.6 Projects

There are many projects in the United States dedicated to embedded technology. Most projects are undertaken by universities and industry, often with support from federal funding agencies such as DARPA, NSF, NASA, etc.

Smart Dust was a project at the University of California at Berkeley supported by the DARPA, among others. The project started in 1997 and finished in 2001,[42] but many additional projects have grown out of it. The project developed tiny sensors, dubbed "smart dust", or motes, with wireless connectivity capable of organising themselves into flexible networks. The aim was to develop a complete sensor network node, including power supply, processor, sensor and communications, in a single cubic millimetre.

While the Center for Embedded Networked Sensing (CENS) at UCLA is not a project itself, rather it is an NSF-funded science and technology centre, many specific projects are carried out at or under the auspices of the centre.[43] Although most of its research is technical, CENS is also studying the ethical, legal and social implications of the new

[40] www.projectliberty.org
[41] www.truste.org
[42] http://robotics.eecs.berkeley.edu/~pister/SmartDust/
[43] The centre received a grant of $40 million over 10 years from the NSF in August 2002. The centre director is Deborah Estrin who led the *Embedded Everywhere* study published by the National Academy of Sciences in 2001. Industry partners include Intel, Sun, Xerox, Cisco, Crossbow, WindRiver, ST Microelectronics, and TRW. The centre's website is www.cens.ucla.edu.

technology. CENS researchers believe that not only is it possible to embed values in the design of information technologies, it is impossible not to do so.

The Portolano project[44] at the University of Washington is tagged as "An Expedition into Invisible Computing". Invisible computing is a term coined by Donald Norman to describe the coming age of ubiquitous task-specific computing devices.[45] The devices are so highly optimised to particular tasks that they blend into the world and require little technical knowledge on the part of their users. The Portolano project, with funding from DARPA, is researching how to make computing devices ubiquitous, to make computer electronics and computation an integral part of all manufactured goods. The UW researchers believe that "reconfigurable computing" will replace dedicated hardware with robust, multi-use electronics.

The AURA project[46] at Carnegie Mellon University (CMU) aimed "to provide each user with an invisible halo of computing and information services that persists regardless of location." The AURA project set out to design, deploy and evaluate a large-scale system demonstrating the concept of a "personal information aura" that spans wearable, handheld, desktop and infrastructure computers. When a user moves from one environment to another, AURA attempts to reconfigure the new environment so that the user can continue working on tasks started elsewhere.[47] AURA was a large umbrella project which, among other things, dealt with security and privacy topics, including caching trust rather than content, establishing trust in surrogates and selective control of location information.

Another important project dealing with trust is called, appropriately enough, TRUST, which is the acronym for Team for Research in Ubiquitous Secure Technology, a project led by the University of California at Berkeley, with partners from nine universities and 11 big companies, including Bellsouth, Cisco, HP, IBM, Intel, Microsoft, Sun, and ESCHER (a research consortium which includes Boeing, General Motors and Raytheon). The National Science Foundation (NSF) is contributing $19 million[48], with the possibility of a five-year, $20 m extension. Additional funding comes from the other partners. TRUST has proposed new software technology that would allow computers to determine whether a program is trustworthy and will do what it claims to do. In addition to protecting computers against attacks, TRUST will consider ways to ensure that stored data remains intact and computer networks keep systems running properly even when intrusions occur – a concept known as "degrading gracefully under attack".

---

[44] http://portolano.cs.washington.edu.

[45] In his 1998 book, *The Invisible Computer*, Norman says computer and technology companies are too focused on the technology, whereas he wants these companies to think about human beings first. In his vision, the computer and its software would fade into the background, become "invisible" and be replaced with simple, task-centred devices.

[46] The project started in year 2000 and continues. It is a campus-wide project. Some funding for the project came from DARPA. www-2.cs.cmu.edu/~aura.

[47] Garlan, D., D. Siewiorek, A. Smailagic and P. Steenkiste, "Project Aura: Toward Distraction-Free Pervasive Computing", in *IEEE Pervasive Computing* 21, No. 2, 2002, pp. 22-31.

[48] The award was announced in April 2005. www.nsf.gov/news/news_summ.jsp?cntn_id=103178&org=NSF&from=news. See also the press release from Berkeley at www.berkeley.edu/news/media/releases/2005/04/11_trust.shtml

## 3.4 UBIQUITOUS NETWORKING IN JAPAN

As in Europe and the United States, the development of a ubiquitous network society can be truly said to be a national strategy. Considerable effort and resources are being invested in realising the strategy from all sectors, governmental, industry, academic.

### 3.4.1 Visions

Japan's vision of or strategy for a ubiquitous network society has been shaped by, especially, three documents (or rather sets of documents). The first are the NRI Papers produced by the Nomura Research Institute. The Ministry of Internal Affairs and Communications (MIC)[49] chose an NRI managing director, Teruyasu Murakami, to chair the policy roundtable which generated the December 2004 report on which Japan's current ubiquitous network society strategy is based. In addition to the NRI Papers and the MIC's own reports, the Mobile IT Forum produced a vision document, which is also a roadmap and a platform, all rolled into one, called the *Flying Carpet* report.

*The NRI Papers*

Nomura Research Institute (NRI) has published about a dozen papers on ubiquitous networking in Japan, including one entitled "Establishing the Ubiquitous Network Environment in Japan – from e-Japan to u-Japan", published in July 2003. In this paper, Teruyasu Murakami proposes a u-Japan strategy. Murakami distinguishes between the concept of ubiquitous computing, as coined by Mark Weiser, and his concept of ubiquitous networking. In the instance of the former, he concludes that physical computers are hidden in the background and people are not necessarily aware of their presence, while with ubiquitous networking, its fundamental basis is the idea of better person-to-person connecting (as well as person-to-object and object-to-object networking). Murakami distinguishes two phases in ubiquitous networking (I and II). In the first phase, the network is "highly vulnerable from the viewpoint of security". The routes for potential security breaches are many and diverse. Only after overcoming this vulnerability do we arrive at Ubiquitous Network II.

*The Flying Carpet*

The Flying Carpet report[50] was produced by the Mobile IT Forum. The first version came out in 2001 and a second version in 2004. It visualises how future mobile communication systems (4G for fourth generation) will be used in social activities around 2010. As in Europe and America, mobile communications are envisaged as integral part of the ubiquitous network society. The report says 4G mobile systems will not only serve as media for communications, but also provide means for connecting users with home appliances and various systems via the home network, etc. In other words, the system itself

[49] The Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) changed its English name in Sept 2004. Website: www.soumu.go.jp/english/index.html

[50] Kato, U., T. Hayashi, N. Umeda et al (eds.), *Flying Carpet: Towards the 4th Generation Mobile Communications Systems*, Ver. 2.00, 4th Generation Mobile Communications Committee, 2004. Flying Carpet was chosen for the report's name because the authors thought "with its magical power to fly the sky, we might be able to foresee our new lives and the underlying mobile technologies a decade from now". See www.mitf.org/public_e/archives/index.html

is required to function as a highly advanced interface system. In a ubiquitous network environment, it says, any product or device may become an object of communications.[51]

Security, privacy and related issues get some coverage in the report, but not in much detail. The report does say that it is "extremely important to implement all possible measures in the system for the protection of personal information."[52] It also says it is necessary to prevent new social problems such as privacy infringement or the abuse of mobile communications for criminal purposes, etc. While countermeasures for these issues should be studied sufficiently by telecom carriers, content providers and service providers, some measures should be undertaken as part of the social environment. For instance, it will be necessary to create a legal structure that could be "strictly" applied to network crimes.

*u-Japan*

The Japanese government has embraced the notion of ubiquitous networking, the Japanese buzz phrase equivalent to ambient intelligence, and has set a target date for achieving it. The u-Japan policy is built on three pillars or goals:
1. Preparation of ubiquitous networks
2. Advanced use of ICT
3. Preparation of an environment for ICT use.

The government has released a u-Japan roadmap. Policy measures will be steadily implemented and all stakeholders encouraged to contribute to the u-Japan strategy. More details of the government's strategy to achieve the u-Japan vision can be found in an MIC White Paper, published in 2004, with the somewhat grandiose title "Building a Ubiquitous Network Society That Spreads Throughout the World".[53]

The White Paper provides an indication of people's expectations of ubiquitous networks generated from a survey.[54] Both individuals and businesses believe that ensuring information security including the protection of personal information is the most important issue. The survey found that the most frequently mentioned concern regarding the use of ubiquitous networks was "fraud and unscrupulous methods of business" followed by "leaks and improper use of personal information in the possession of businesses" and "improper access to and use of personal information".[55]

The high level of public concern about the issue of protection of personal information was reflected in (or perhaps stoked by) press reports. The number of reports of incidents involving personal information has been increasing. In February 2004, there was an incident in which the personal information of approximately 4.5 million subscribers including names, addresses, telephone numbers, and e-mail addresses in the possession of a major telecommunications carrier was leaked.[56]

---

[51] Kato et al, p. 60.
[52] Kato et al, p. 50.
[53] MPHPT, Information and Communications in Japan: *Building a Ubiquitous Network Society that Spreads Throughout the World*, White Paper, Ministry of Public Management Home Affairs Posts and Telecommunications of Japan, Economic Research Office, General Policy Division, Tokyo, 2004. http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2004/2004-index.html
[54] MPHPT 2004, p. 18.
[55] MPHPT 2004, p. 31.
[56] MPHPT 2004, p. 32.

On the other hand, the survey found that only a small percentage of individuals take any measures to protect personal information. Interestingly, of individuals who do not take any measures, many said they do not know of any specific measures to take. The survey found that even among businesses, many do not take any specific system and technological measures to protect data nor any organisational and structural measures.

### 3.4.2 Scenarios

From research done to date, few scenarios appear in papers about Japan's ubiquitous networking projects, at least, not scenarios developed to the extent that one finds in (especially) European and American projects. However, that does not mean scenarios are absent. The Smart Hot-Spot project (see below) has a couple of relatively simple undeveloped scenarios, which show use of smart furniture in daily life, one in the home and one at a train station.[57]

Not all scenarios need to be written, of course. The Ministry of Internal Affairs and Communications prepared a briefing package for the overseas press which has several "images" of the ubiquitous network society. On KDDI's website, one can find several ubiquitous network scenarios in video format.[58]

### 3.4.3 Roadmaps

The comment about the relative scarcity of scenarios in Japan also applies to roadmaps. Where in Europe the use of roadmaps is relatively common, they are almost absent (or at least not very visible in documents translated into English) in Japan.

Two notable exceptions are the roadmaps mentioned in the Flying Carpet report and in the MIC's White Paper. In order to steadily implement the u-Japan Policy, MIC has developed a roadmap identifying 31 items having a specific schedule and realisation of the objectives by 2010.[59]

### 3.4.4 Research agendas

The *Flying Carpet* report is not only a vision document, it's also a research agenda. So, to a lesser extent, is the MIC's White Paper. Apart from those two documents, and the company-specific research agendas of corporate Japan, one could say that, to some extent, research agendas are being set by the various research laboratories, especially in universities, working on ubiquitous network society solutions. There are many such research laboratories, including the Aoyama-Morikawa Laboratory (AML)[60] at the University of Tokyo, the Hide Tokuda Laboratory at Keio University[61], the Ubiquitous Computing Laboratory (UbiLab)[62], the YRP Ubiquitous Networking Laboratory (YRP

---

[57] Ito, M., A. Iwaya, M. Saito et al., "Smart Furniture: Improvising Ubiquitous Hot-spot Environment" in *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops* (ICDCSW'03), Providence, RI, 19–22 May 2003, IEEE Press, 2003, pp. 48-53.
[58] See the "Knock! Knock! Ubiquitous" video streaming scenarios at www.kddi.com/english/index.html
[59] Ninomiya, S., "Policy and Regulatory Update by Japan" in APEC Telecommunications and Information Working Group, 31st Meeting, Bangkok, 3-8 April 2005.
[60] www.mlab.t.u-tokyo.ac.jp
[61] www.ht.sfc.keio.ac.jp
[62] www.ubi-lab.org. UbiLab is an undertaking of Keio University and others.

UNL)[63], the Ubiquitous Networking Laboratory (UNL)[64] and the Distributed and Ubiquitous Computing Laboratory at Waseda University in Tokyo[65].

### 3.4.5 Platforms

From the research done so far, we have discovered few or no analogues in Japan to the platforms one finds in Europe, that is to say, platforms which draw together industry, governments, regulatory authorities, universities, financing bodies, standardisation bodies and other stakeholders. The platforms, such as they are, in Japan tend to be composed of industry full stop. This is not to say that the various stakeholders do not collaborate. They do, but in a different way. The Ministry of Internal Affairs and Communications, for example, will often initiate study groups, committees, councils and so forth, primarily composed of industry representatives, to provide advice and recommendations to the Ministry. Industry-composed groupings do not wait to be called upon to provide advice. They also make recommendations to the government. They also, as in Europe, attempt to achieve standardisation, not always successfully. Among the "platforms" working on the ubiquitous future are the following:

The Ubiquitous Networking Forum[66] was established in 2002. Its aim is to realise ubiquitous networking at an early date, engage in research and development, standardisation, surveys, liaison and co-ordination with other organisations. In February 2004, the Ubiquitous Networking Forum released a document about RFID trials in Japan. The document, entitled "Best Practices", describes 14 RFID trials and applications in supply chains, logistics, baggage tracking at airports, food traceability, tracking children, office work support, fire and disaster prevention / rescue, location systems, manufacturing.

The Mobile IT Forum (mITF)[67] was created in 2001 to work towards realisation of the fourth-generation mobile communications systems and mobile commerce services. Its activities include R&D, standardisation and spectrum studies, co-ordination with related bodies, collecting information, and carrying out promotional and educational activities. Its most significant output, available in English, is the *Flying Carpet* report (see above). As of 2002, it had more than 120 members, primarily from industry.

The TRON Association takes its TRON acronym from "The Real-time Operating system Nucleus." The initiative for its formation came from University of Tokyo professor Dr. Ken Sakamura who in 1984 dreamed up the TRON concept as a new computer operating system architecture. He encouraged industry and academia to collaborate on its development as a standard and its introduction into the computing market. The TRON Kyogikai was formed in 1986 to oversee the project, and this body became the TRON Association in 1988.[68] Membership in the TRON Association is open to anyone who shares in the objectives of the TRON Project.

---

[63] YRP is the abbreviation for Yokosuka telecom Research Park. www.ubin.jp/english/aboutus.html.
[64] The UNL at Tokyo Denki University (www.unl.im.dendai.ac.jp/index.html) should not be confused with the YRP UNL.
[65] http://www.dcl.info.waseda.ac.jp/home/index.html.en
[66] www.ubiquitous-forum.jp (in Japanese only)
[67] www.mitf.org
[68] www.tron.org

The TRON Association's vision is of a "computing everywhere" environment in which objects are embedded with computer intelligence and able to communicate with each other. The results of the TRON Project are made available as open specifications.

The T-Engine Forum is a non-profit voluntary organisation formed in 2002, as an initiative of five Japanese chipmakers and 17 other Japanese tech firms.[69] As of May 2005, the body had 448 members. T-Engine has been described as "arguably the most advanced ubiquitous computing platform in the world".[70] The forum collaborates in developing ubiquitous computing solutions using off-the-shelf components. The instigator of T-Engine and its chairman is the ubiquitous Prof. Sakamura (see above).

The Ubiquitous ID Center was set up in March 2003 and operates within the T-Engine Forum. It promotes research and development, standardisation and diffusion of ubiquitous computing and networking technologies for automatically identifying physical objects and locations. As of end 2004, the uID Center had 470 member companies.[71] The uID Center claims to hold the world's most advanced technologies in the fields of small devices and small-sized electronic devices. The Japanese Ministry of Land, Infrastructure, and Transport is testing one of the uID Center systems in a project where electronic tags are embedded in pavement stones and street furniture which will supply users with location-specific information "anytime, anywhere, to anyone."

The Ubiquitous Service Platform is an initiative of NTT Data Corp, Fujitsu, NEC and Hitachi who, in April 2005, announced an agreement to investigate a ubiquitous service platform that can seamlessly link diverse IT systems and equipment using ID as a linkage key.[72]

A similar initiative has been undertaken by IBM, Intel and NTT DoCoMo who set up a Trusted Mobile Platform based on specifications that define security features for mobile devices.[73]

The Communications and Information network Association of Japan (CIAJ)[74] is an industry association established in 1948. It 300 member companies are either producers or users of information-communication technologies and/or services. CIAJ has numerous committees and working groups which make policy proposals, create new business opportunities, provide information and tackle industry-wide issues such as environmental concerns and interoperability. Several of its committees and working groups deal with issues directly related to the ubiquitous network society.

The Electronic Commerce Promotion Council of Japan (ECOM)[75] was established in 2000 to promote electronic commerce and to make recommendations to the government to achieve secure electronic commerce, to establish international standards based on user needs, and make international contributions in this field. The old ECOM was superseded

[69] Its website is www.t-engine.org/english
[70] Krikke, J., "T-Engine: Japan's Ubiquitous Computing Architecture Is Ready for Prime Time", in *Pervasive Computing* 4, No. 2, 2005, pp. 4-9.
[71] The Chairman of the uID Center is Dr Ken Sakamura. Its website is www.uidcenter.org/english/introduction.html
[72] www.nttdata.co.jp/en/media/2005/042000.html
[73] www.trusted-mobile.org
[74] www.ciaj.or.jp/e/index.htm
[75] www.ecom.jp/ecom_e/index.html

by a new industry organisation called Next Generation Electronic Commerce Promotion Council of Japan. The old acronym ECOM was, however, retained in view of its recognition in Japan and abroad. ECOM industry members include Hitachi, IBM Japan, Matsushita, Microsoft, Mitsubishi, NEC, Nomura, NTT, Toshiba and Toyota. Among the various activities undertaken by ECOM are several relating to security, encryption, authentication, protection of privacy and consumer protection.

### 3.4.6 Projects

There are quite a few ubiquitous network projects in Japan. Little information is available on the sources and amounts of funding. Many of the projects have been undertaken by the laboratories mentioned in the research agenda section above. There seems to be no projects on the scale of the largest European and American projects and none with large consortia of partners, as one finds in America and especially Europe. Furthermore, none of the projects has been specifically dedicated to privacy, security, identity, trust and the digital divide. Nonetheless, protection of personal information and security are of concern to the Japanese and these issues are frequently mentioned in the projects and other documents.

Among the main ubiquitous network society projects are the following:

The Ubila project[76], sponsored by the Ministry of Internal Affairs and Communications (MIC) of Japan in co-operation with industry, academia and government, aims to realise ubiquitous networking, where computers and networks are present in all aspects of daily life. Its specific focus is on control management technologies for ubiquitous networks.

Project STONE was initiated at the University of Tokyo in 1999 (and is continuing) to develop an innovative network architecture for supporting future ubiquitous computing applications. STONE provides service discovery, context awareness, service synthesis, and service mobility.[77] The STONE project developed an authentication process so that even appliances could establish the identity of different users. Authentication of appliances also were designed to prevent impersonation attacks on the network. In the project, all communications over the network were encrypted by secure sockets layer (SSL) encryption to make the system resistant to tampering.

The official name of the Yaoyorozu project (Aug 2002-Mar 2005)[78] is "Research on Ubiquitous Information Society based on Trans-Disciplinary Science". The project has several partners including Hitachi, the University of Tokyo, Keio University, the National Institute of Media Education and Tokyo University of Technology and UDIT. It has received support from the Ministry of Education, Culture, Sports, Science and Technology (MEXT). Its principal research goal is desirable institutional systems and core technology for the ubiquitous information society in 2010. The Yaoyorozu project, for example, is asking questions about whether existing privacy protections are sufficient. The teams are examining ethics in the ubiquitous information society, increasing privacy consciousness as well as enhancing secure and versatile connectivity. One of the project's four themes is

[76] Participants include the University of Tokyo, Kyushu Institute of Techology, NEC Corporation, Fujitsu Limited, KDDI R&D Laboratories Inc., KDDI Corporation. www.ubila.org

[77] Kawahara, Y., M. Minami, S. Saruwatari et al, "Challenges and Lessons Learned in Building a Practical Smart Space", in *The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, Boston, MA., 22-26 August 2004, pp. 213- 222.

[78] The project's website is www.8mg.jp/en/outline_goals01.htm.

the examination of appropriate policies for handling privacy and clarifying the basic requirements.

# 4 ANALYSIS OF EXISTING AMI SCENARIOS

This chapter presents an analysis of existing AmI scenarios in which AmI technologies are used in everyday life. A review was made of more than 60 project and roadmap scenarios and research publications with the goal of understanding how they might change our lives. The vision of a future everyday life is a mixture of many diverse applications clustered in the following domains: home, work, learning, health, shopping and mobility. In our analysis, we present the main application domains and their visions, and then list the main benefits and threats identified in the scenarios, open issues and our conclusions.

## 4.1 CONSTRUCTING SCENARIOS

Constructing scenarios is a way to present in a concise form the most visible research activities in a certain application domain. AmI application scenarios can be found in many different forms.

- First, there are elaborated scenarios (screenplays) with actors and their activities, with many details and a well-defined storyline. These scenarios can be either purely conceptional, theoretical visions of a future such as the ISTAG scenarios[79] or scenarios developed by projects to present a project goal. In the latter case, the scenario is likely to describe the system or technology prototype which is to be built and evaluated during the project, although there might be modifications.
- Second, there are application scenarios which usually concentrate on a certain functionality of a system prototype. The storyline in these scenarios is detailed only in parts which describe the system functionality.
- The third and most common type of AmI application descriptions are not even called scenarios and don't present any storylines. The application scenario is hidden behind the description of system functionality. Such descriptions often suggest interesting application areas which one may not find in more elaborated scenarios; moreover they are not pure visions, they are working prototypes.

One can depict the role of scenarios as follows:

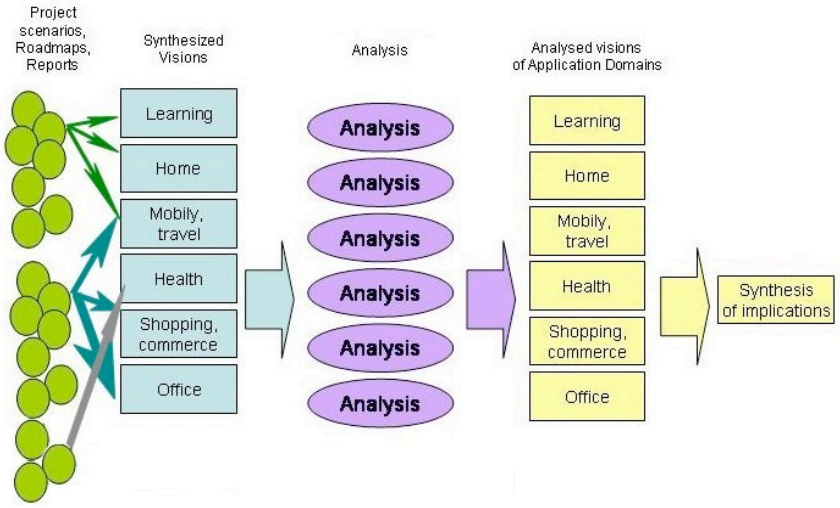


*Figure 2: Analytical Framework*

[79] IST Advisory Group, K. Ducatel, M. Bogdanowicz et al., *Scenarios for Ambient Intelligence in 2010*, EUR 19763 EN, EC-JRC, Institute for Prospective Technological Studies (IPTS), Sevilla, 2001. http://www.cordis.lu/ist/istag-reports.html.

The SWAMI partners have synthesised future visions from the material we reviewed, including the well-known ISTAG scenarios as well as scenarios developed in the context of the the ITEA Technology Roadmap for Software-Intensive Systems[80] and various projects including especially the AMSD[81], COCONET[82], MIMOSA[83], Smart-Its, 2WEAR[84], CANDELA[85], Amigo[86], MiMe[87] InterLiving[88], ACCORD[89], RUNES[90], and Oresteja[91] projects.

Our synthesised visions are not presented as a storyline, but as a list of people's activities supported by AmI. Our synthesis provides for a structured view and is, we think, easy to grasp. We decided to pay special attention to the following dimensions:

- available information about the personality of the main actor in a given scenario, because social and privacy issues depend on the scenario target, e.g., people with disabilities may be willing to exchange some privacy to get more support; and very small children don't care about privacy yet;
- the environment where the scenario takes place, because people have different expectations about privacy in different environments, e.g., in their own home and in nature people are less willing to accept the same behaviour restrictions as in public places;
- the activity described in the scenario, because activity is an important part of a personal context and because information flow is closely linked to the activity;
- information flow in the scenario, because many privacy threats are associated with disclosure of information. Information storage and exchange present different threats and different means to avoid them are needed;
- AmI control level vs. a person's control level. AmI has a high control level when it acts on behalf of a person, e.g., it decides to reject a phone call or to forego transmission of personal information. AmI has a medium control level when it gives advice, e.g., to reduce car speed due to a road bend ahead. AmI has a low control level when it only executes a person's command. This dimension is important because the high control

---

[80] ITEA *Technology Roadmap for Software-Intensive Systems*, 2nd edition, Information Technology for European Advancement (ITEA) Office Association, Eindhoven, 2004. www.itea-office.org

[81] AMSD is the abbreviation for Accompanying Measure System Dependability. The project (June 2002-August 2003) had a budget of €399,979 and six partners. Its website is https://rami.jrc.it/roadmaps/amsd

[82] Aschmoneit, P. and M. Höbig, *Context-Aware Collaborative Environments for Next Generation Business Networks: Scenario Document*, COCONET deliverable D 2.2, Telematica Institute, Enschede, 2002. http://www.mosaic-network.org/library/scenarios.html

[83] Kaasinen, E., K. Rentto, V. Ikonen and P. Välkkynen, *MIMOSA Initial Usage Scenarios*, MIMOSA Deliverable D1.1, version 1.0, 2004. http://www.mimosa-fp6.com/cgi-bin/WebObjects/MIMOSA.woa/1/wo/g6hDj8CHIFBQDjTQXuNVGM/8.0.5.11.

[84] Savidis, A., S. Lalis, A. Karypidis et al, *Report on Key Reference Scenarios*, 2WEAR Deliverable D1, Foundation for Research and Technology Hellas, Institute of Computer Science, Heraklion, 2001.

[85] Sachinopoulou, A., S. Mäkelä, S. Järvinen, et al., "Personal video retrieval and browsing for mobile users" in *17th International Symposium Electronic Imaging Science and Technology*, San José, CA, 16-20 January 2005.

[86] http://www.hitech-projects.com/euprojects/amigo/
http://www.ctit.utwente.nl/research/projects/telematics/other/amigo.doc/

[87] http://www.mimeproject.org

[88] http://interliving.kth.se

[89] Åkesson, K.-P., J. Humble, A. Crabtree, A. and A. Bullock, *Usage and Development Scenarios for the Tangible Toolbox*, ACCORD Deliverable D1.3, Swedish Institute of Computer Science, Kista, 2001.

[90] http://www.ist-runes.org

[91] Palmas, G., N. Tsapatsoulis, B. Apolloni et al., *Generic Artefacts Specification and Acceptance Criteria*, Oresteia Deliverable D01, STMicroelectronics s.r.l., Milan, 2001.

level of AmI, first, makes it easier to obtain personal to obtain personal information by hacking or controlling AmI technology; second, leads to higher dependence on AmI; third, affects humans' acceptance of AmI and last, raises a lot of questions about legal responsibility (when AmI makes a decision, who is legally responsible for it?);

- enabling technology (including details about how an AmI system was envisioned to work in the original source) because many privacy threats are associated with system implementation. For example, in the AMSD project[92], one of the scenarios contains a statement: "The agent knows the preferences of Elena's friends since they have earlier been to Elena's place." We think that "since they have earlier been to Elena's place" is an important scenario element because it indicates that information is stored somewhere in the system.

## 4.2 HOME APPLICATION DOMAIN

As a person's most private place, the home needs to be designed carefully because the home atmosphere is important for personal happiness and development. If a spy wants sensitive personal information about somebody, the best way to get it is to observe that person at home. Many financial and private affairs are discussed or dealt with from home; personal vulnerabilities, strengths and health problems can be seen easily. Second, people perceive their homes as a place where they can be free from intrusion, relax and think in peace, i.e., "to be let alone". As Nissenbaum said, this privacy aspect is very important for personal development.[93]

Many AmI projects and roadmap scenarios support home activities such as the following:

- communications, both between inhabitants and between people inside and outside the home. Unlike communications over the Internet, where people often communicate with complete strangers and can present virtual personalities very different from their real ones, the communications envisaged in future homes mainly provide connections between friends, family members and relatives. This means transmitting real personal data in large quantities. Communications are often envisioned to happen via video link, sometimes "always on". Several AmI scenarios describe how parents check what children are doing by initiating a visual link;
- providing personalised access to external information of all kinds;
- providing reminders about coming events, which things to take, which shoes to put on, which food products to buy, how to clean teeth, how to cook and even reminders to drink less or to be more polite (based on physiological assessments during conversations, especially phone calls);
- finding personal belongings, e.g., toys or lost keys;
- controlling appliances (from lights, fridges and washing machines to automatic doors with access control) and other household objects (including clothes, keys and food products) to make household duties and maintenance tasks easier, and to provide remote access to the home;
- increasing safety and security by tracking people, appliances and objects; preventing or fast reporting of accidents; access control;
- entertainment and increasing comfort levels.

[92] Masera, M. and R. Bloomfeld, *A Dependability Roadmap for the Information Society in Europe*, AMSD Delilverable D1.1, 2003. https://rami.jrc.it/roadmaps/amsd.

[93] Nissenbaum, H., "Privacy as Contextual Integrity", in *Washington Law Review* 79, No. 1, 2004, pp. 101-139.

Most scenarios describe homes independently from their locations (i.e., there is no indication whether the home is located in an urban or rural area). Thus, the future home is assumed to be a complex system, an environment capable of sophisticated interactions with its inhabitants, and the supporting infrastructure is assumed to be present everywhere.

Home is a private sphere which can become semi-public when visitors arrive. However, with the increasing connectivity between people at home and outside the home and between the home and other spaces, such as organisations and homes of other people, there is a danger that the home space becomes less private than it used to be. Indeed, if there is a video connection between two rooms of a home, e.g., a child's room and a kitchen, how can a child perceive her own room as a private space? And if parents can see from their workplaces what the child is doing when alone at home, this means that a child is never left alone. Another aspect of this trend is increasing opportunities for surveillance and spying on people at home via the home's connections with the outside world, and even to control home appliances from outside in a way not really desirable by home inhabitants, e.g., to arrange arson remotely.

Another trend is to augmet everyday objects with communications and computer capabilities. This implies that it becomes more difficult to hide personal belongings, e.g., things which were just bought and their prices, from other family members, which reduces privacy at home.

### 4.3 WORK APPLICATION DOMAIN

The work domain has three noteworthy aspects: first, people spend a lot of time working, but they are less free to choose their working environment than their home environment. If organisations choose to violate personal privacy in some way, workers can either accept it or try to find a better employer. In any case, if workers feel their privacy is violated, they can feel humiliated and depressed, and it is an open question how much an organisation will benefit or lose from close surveillance of its employees.

Second, people can not avoid dealing with some personal matters during working hours, e.g., making appointments to see a doctor or a teacher of their children; talking to a mechanic about repairs to their cars; communicating with family members; reserving a table at a restaurant and so on. It is difficult to avoid doing some personal things because working hours are more or less the same everywhere and children may need parental permission or advice during working hours. Thus, it follows that intellectual property is not the only thing which should be protected in a working environment. Personal affairs also need to be protected.

Third, our analysis of research projects targeted at developing AmI at work has shown that visions of the future working environment are already being implemented in some companies, hospitals and research institutes. Thus, we can expect to work in a smart environment sooner than to live in a smart home. Consequently, safeguards of privacy at work should be developed as soon as possible.

From the scenarios we reviewed, AmI will support future work environment activities such as the following:

- communications, both between people in the office and between people inside and outside the office, both work-related and non-work-related. Video communications between colleagues, often in an "always-on" mode, are commonly suggested. One important distinction between ongoing projects and future scenarios is that ongoing projects assume that many working meetings are physical meetings of people, and the virtual world provides mainly a means of awareness of colleagues' activity or a means of collective editing of documents, while visions of the future are of more virtual communications. The visions also emphasise the importance of supporting co-operation between different organisations, globalisation and interoperability;
- support for mobility of workers, i.e., the opportunity to work from any location at any time: from home, during a trip or holidays;
- providing access to work-related information at any time and from any location, improving knowledge sharing and co-operation;
- providing efficient working tools, e.g., powerful simulators and tools for handling documentation, including multimedia recordings of meetings;
- controlling diverse working appliances, e.g., projectors and screens, turning the whole office environment (including halls and corridors) into a smart space capable of tracking people, contacting them and memorising their work;
- increasing safety and security, depending on work requirements;
- giving reminders and planning agendas;
- domain-specific functionalities such as diagnostics of equipment, factory automation, dynamic pricing of goods, warehouse management, etc.

Like the AmI-enabled future home, the office environment is assumed to be a complex system capable of sophisticated interactions with workers, and the supporting AmI infrastructure is assumed to be present everywhere. With communications (satellite and terrestrial) available virtually everywhere in the world, employees can be reached wherever they are and they, in turn, can access their office from virtually anywhere – i.e., it is almost impossible to "escape" from work. The office environment is generally a public place, but even so, employees (especially those having their own office) often perceive "their" office or cubicle as semi-private with fewer behavioural constraints than in a purely public space. This semi-private character applies also to chat with colleagues in corridors and coffee rooms.

## 4.4 HEALTH APPLICATION DOMAIN

The health domain has two aspects: on the one hand, health care determines the life and death of people, and fast access to a person's health information (e.g., allergies and chronic diseases) can be very important in case of emergency. On the other hand, health information is highly sensitive. People may be unwilling to reveal their health problems even to close relatives, let alone to work superiors or insurance companies. Thus, it is important (but maybe not so easy) to build AmI applications in the health domain so that emergency workers and doctors can access personal information whenever needed, but nobody else can do so without authorisation.

The main AmI functionalities in the health domain are the following:
- prevention of diseases, which includes continuous monitoring of health and health-related behaviour (e.g., sports exercises); promotion of healthy lifestyle and related

advice; alerts against eating dangerous products (e.g., those which can cause allergic reactions); and prediction of diseases, e.g., by gene analysis;

- curing diseases, which starts from diagnosis (by video link and so-called "lab on a chip" technologies for measuring blood pressure, urine tests, etc) and continues as a treatment at any time and any place. This should be achieved by ad hoc networks of medical equipment and information sharing between doctors, and by tiny AmI systems capable of drug delivery, e.g., implantable insulin dispensers for diabetic patients. AmI systems should be also capable of automatic diagnosis of an emergency and giving the necessary medication, e.g., in case of heart problems and epilepsy. In these cases, continuous monitoring is also needed;
- care, which is a long-term activity directed towards the recovery process of patients and towards the support of everyday life functions of people in need of long-term attention, such as the elderly, handicapped or chronically ill. Care also implies continuous monitoring, by means of embedded intelligence capable of tracking activities, detecting anomalies and giving advice inoffensively; and so-called assisting technology such as hearing aids, prostheses and implants (e.g., heart implants);
- optimising the alarm chain in case of an emergency (e.g., heart attack or an accident), from calling for help to preparing treatment;
- support functions, e.g., improving information exchange, helping to select the right specialist or to use insurance.

Thus, health applications are envisioned as becoming possible at any place and any time, with sophisticated embedded sensors and/or actuators continuously tracking the individual's actions and health.

## 4.5 SHOPPING APPLICATION DOMAIN

Ambient intelligence applications in shopping and commerce aim to create a user-friendly, efficient and distributed service support to the customer, such as managing his or her search for and selection of merchandisers, and handling order and payment processes. A commercial transaction covers a complex range of activities from the moment a customer enters a shop to product selection, purchase, billing, shipping and possible return of merchandise. The main AmI-enabled services provided to a customer are the following:

- personal shopping management by compiling items for purchase by intelligently surveying the stocks of food and other goods in the household and linking them intelligently with information about the customer's preferences and habits (customer profiles);
- the AmI-enabled store lets shoppers find and select items for purchase by using intelligent tags for goods and intelligent terminal devices for the customer (in shopping carts and mobile personal devices) and for the shop owner (intelligent cash register). It may include a gift registry, wish or purchase lists, and has the ability to save a record of shopping cart contents between visits on a personal device;
- order processing manages payment, including tax calculation and credit card transactions. It also includes functions such as management of customers' addresses, discount and coupon application, inventory processing and delivery.

Similar to other application domains, shopping is envisioned to be possible as a remote activity from any place and at any time. Scenarios that describe shopping by someone's physically visiting shops don't specify shop locations, thus implying that shops can be found everywhere. Scenarios of "order and delivery" imply the presence of a delivery

infrastructure, which is more likely to be developed first in urban areas, although scenarios don't mention it explicitly.

## 4.6 LEARNING APPLICATION DOMAIN

At the Lisbon European Council in March 2000, government leaders set the EU a 10-year mission to become the most competitive and dynamic knowledge-based economy in the world, capable of sustained economic growth with more and better jobs and greater social cohesion. Lifelong learning is a core element of this strategy. The aim is to make lifelong learning a reality for all from any place, at any time and at the individual's own pace, promoting learning for personal, civic and social purposes as well as for employment-related purposes.

AmI should support the following activities:

- intentional learning, i.e., by taking courses either in a classroom or remotely. The main emphasis is on presentation of learning material (visualisation, gaming, augmented and virtual reality, etc); assessment of a learner's progress and adjusting the material presentation and pace of learning to individual needs and capabilities; promotion of collaborative learning since a social element in learning increases efficiency and enjoyment of learning;
- reducing teacher workload by helping in planning, preparation of presentations, logging of personal learning history, and even giving homework, assessing it and controlling the whole learning process as illustrated in the ISTAG scenario "Annette and Solomon";
- informal learning, i.e., by experience, either one's own or shared with somebody else. This is often mentioned in the context of work and learning for work; and in the context of learning by children, where AmI makes experiences richer by digital augmentation of physical objects and by making toys intelligent;
- learning by diverse groups of people, from ethnic minorities to people with disabilities.

Learning takes place in a variety of environments in and outside the formal education and training system and is envisioned as a continuous process.

## 4.7 MOBILITY APPLICATION DOMAIN

In its technology roadmap on Software Intensive Systems, ITEA has developed a vision of what it describes as the nomadic domain. In the ITEA vision, the nomadic domain will have the same facilities and services as those in the home and at work, but while people are at different places temporarily or on the move (e.g., on the road). The mobility domain has two aspects: first, people are not free to control the environment where they move – governments require passports, visas, driving licences, etc; transportation companies have rules too, e.g., where to put the luggage and what can or can not be transported. AmI technologies are already becoming present in the mobility domain in the form of biometric passports, supported by governmental financing, which will soon become obligatory in Europe.

Second, people travel both for work and for their own pleasure. Travel is an important feature of life today. This means that privacy protection in the mobility domain needs to be

developed urgently, otherwise travellers will be left with the choice either of accepting threats to their privacy or ceasing to travel (and for those who travel for work, ceasing travel is simply impossible).

AmI is envisioned as supporting the following in the mobility domain:

- various kinds of communications, e.g., between family members located in different places and between strangers located in the same place. Unlike the home domain, video communications between parents and their children can be independently initiated by adults or children. Typical connections in mobility travel scenarios consist of remote access and communications with home, work and people (friends and family);
- access to all kinds of information (home, work, health, infotainment, weather, etc);
- efficient intelligent transportation systems (timely, accurate, personalised traffic information available on the spot);
- safety: for pedestrians by AmI detecting cars; for cars by automated driving and detection of a driver's state; and generally by monitoring the environment and detection of events and accidents which might affect travel;
- fast payment of road tolls, tickets and other travel fees;
- help in emergencies, e.g., by locating casualties quickly and informing authorities about their conditions;
- increasing comfort and pleasure;
- all kinds of access control, from access to rental cars to border crossing; also controlling the information about whether a person is available or not;
- environmental protection by controlling the speeds and numbers of cars on the roads.

Although it is envisioned that functionalities available on the move in any environment are similar to those at home or work, the requirements are different, depending on whether the place is fixed (but temporal) or people are moving (e.g., driving a car, walking). Generally, this implies that the environment is neither public nor private, rather it can be semi-private or it can switch between public and private spheres frequently.

## 4.8 Observations about existing AmI scenarios

In addition to the activities supported by AmI and the environment (domain) where the scenario takes place, as described in the preceding sections, we consider the following dimensions as important for scenario analysis in the context of privacy threats and social implications.

### *Actors in scenario activities*

Most of the scenarios we analysed feature ordinary working people (some are in the executive class) without significant health problems, and it is assumed that most people, including the elderly, have embraced AmI. With the exception of scenarios describing support for shopping and everyday activities for elderly people (in most of the scenarios, they live alone), support for such basic everyday activities as shopping, watching TV and waking up by an alarm clock are often described as the activity of a healthy adult.

AmI focused on the individual can create problems in family relations. For example, in scenarios describing how an intelligent TV is able to select only the channels and programs that are really interesting for the user (e.g., by measuring the user's physiological signs), it

is rarely mentioned that there can be several family members with conflicting interests. The ITEA scenario "the Rousseaus' holiday" is one of a few exceptions in this sense. Similarly, shopping scenarios often neglect the fact that shopping is not always an individual experience but also a group activity, where family members often have very different responsibilities and decision rights. With the exception of projects in the learning domain, the roles of children in scenarios are too often restricted to playing games, being checked by parents and receiving reminders to do homework.

Significant attention is devoted to supporting communications between humans. Communications between family members, relatives, friends, colleagues and strangers can be asynchronous (messaging) or synchronous (mainly video communications), at home, at work (both on non-working and working issues) and while moving. However, many scenarios describing communications between adults and children present them in such a way that parents activate the video link in order to check what their children are doing; it is not clear whether the children have rights to avoid being observed.

Health care scenarios and some of projects in the learning domain are different from scenarios in other domains in the sense that they are targeted at people with chronic diseases, health risks, elderly people and people with disabilities. However, the general rule is that a person's problems or disabilities are described only if there is an AmI solution to help them. Most scenarios imply that AmI itself works excellently and does not create problems for people. One of the rare exceptions in this sense is MIMOSA project[94] which has scenarios where AmI advice is not always perfect and where misunderstandings with the AmI system may arise.

Another feature of scenarios describing smart environments (whether it is a smart shop or city-wide ambient intelligence) and basic human activities (such as shopping or going to work) is that they assume that all people have accepted the new technologies.

*AmI control level vs. person control level*

We distinguish three levels of AmI control:
- High: AmI acts on behalf of the person.
- Medium: AmI gives advice and proactive suggestions.
- Low: AmI executes the person's commands.

In most scenarios of modern life and in all scenarios of the distant future, AmI has a high control level over security (in the form of access control to online courses, houses, cars, work, health data, payments, in passports and immigration control) and privacy issues (scenarios don't present explicit user interactions with AmI systems where the user is granted access rights and control over personal data, thus, it is assumed that AmI has high level control over privacy issues).

Applications where a person's life depends on AmI and where AmI has a high level of control include safe mobility, especially driving (AmI detects obstacles, controls car speed and ensures that the car stays on the road), health monitoring and detection of a health crisis (such as a heart attack). The control over car speed is suggested also for environmental reasons. Generally, in driving scenarios, it is not clear if users are free to

[94] Kaasinen, E., K. Rentto, V. Ikonen and P. Välkkynen, *MIMOSA Initial Usage Scenarios*, MIMOSA Deliverable D1.1, version 1.0, 2004. http://www.mimosa-fp6.com/cgi-bin/WebObjects/MIMOSA.woa/1/wo/g6hDj8CHIFBQDjTQXuNVGM/8.0.5.11.

organise their travel means, time and route. Scenarios of future health care raise a question about whether medical monitoring and diagnosis systems are transparent enough for a typical (often elderly) user to gain a full understanding about what kind of data are gathered, where they are stored and transmitted, and what happens to them.

### *Personalisation of services*

An important feature of AmI with a high level of control is personalisation, which can be applied for adjusting an environment (lighting, heating); for filtering of shopping advertisements and selection of TV programs or adjusting learning material to individual capabilities and preferences. For doing these sorts of things, AmI needs to evaluate a learner's progress and in the Oresteia scenario[95], it is proposed to evaluate also the learner's state during learning (bored, frustrated, etc) and to select exercises according to such evaluation. In scenarios such as the "Annette and Solomon" scenario from ISTAG, the AmI control level in teaching and personalisation is very high. Actually, most teaching is performed by AmI, while the human tutor is stated to be "not necessarily very knowledgeable about the subject of study", and whose role in the scenario is not very clear. This raises a question of how people perceive such AmI superiority.

An important question about personalisation is, however, not the degree of AmI vs. personal control, but the question about who is in control of the AmI system. Whether in shopping, or in news filtering, or in recommendations about medicines, trips, etc, how are the user's interests protected and how is it ensured that information is objective? At the moment, privacy protection activists have severe doubts about the customer's control of AmI-enabled shopping services. Since retailers are the owners and operators of AmI infrastructure and provide customer services, one could assume that they would like customers to have as little control over AmI as possible. This might result in customers not wanting to use AmI-enabled services or products at all.

The AmI control level is also high in communications, first of all, because AmI handles connections between numerous different networks and adjusts the contents to user devices. Second, many scenarios describe high control at the application level, e.g., in emergencies where the communication between the ill or injured person, the emergency centre and the various paramedics en-route is completely automated. Manual intervention is only allowed in a few cases and is limited to acknowledgements. The emergency scenario is thus dependent on a well-designed process chain and complete coverage of the country with an AmI infrastructure. Emergency scenarios usually depict rather modest cases where the technology is not severely damaged. It remains open if the emergency system would continue to function properly when major components in the AmI network are destroyed (e.g., in a terrorist attack or by natural catastrophe). Otherwise, this would suggest that, at the least, robust and possibly redundant communication procedures are needed that can also rely on low technology.

### *Information flow in the scenarios*

In most scenarios, the AmI system recognises people, either for the purpose of access control or for personalisation. In many scenarios, it is left open how exactly personal

[95] Palmas, G., N. Tsapatsoulis, B. Apolloni et al., *Generic Artefacts Specification and Acceptance Criteria*, Oresteia Deliverable D01, STMicroelectronics s.r.l., Milan, 2001.

identification is performed, but there are indications that people have either an “identity token” that can be read by the system or that biometrics are used. Both possibilities have identity theft risks associated with them.

Scenarios that require high security (like immigration control, or protection of professional secrets, or access to health data) and that mention biometric sensors don't usually describe which biometrics are used. However, it seems probable that highly reliable biometrics, such as iris scanning or fingerprint reading, will be used in high-security applications, and theft of highly reliable biometrics data is very dangerous. It is worth noting that identity information is always stored somewhere (in a personal device or in a central database or both) and it is always exchanged (transmitted) during the authentication process. The presence of identity information in both forms increases a risk of identity theft, particularly when one takes into account the fact that currently information stored in personal devices is poorly protected.

Another popular element of scenarios is the presence of information about a person's or object’s location and/or destination. Most often, it is processed locally, in the user device or in the car, but it can also be transmitted, e.g., in scenarios describing car-pooling. Scenarios which describe how a navigation system gives advice to select another road due to an accident or traffic jam ahead don't describe how the event is detected, but it seems probable that at least the location of a car in an accident has been transmitted.

Tracking of workers’ location and location of work-related objects (which means again tracking of personal location in cases where a work-related object is used by a particular person) is also seen as a common functionality of AmI, and in such scenarios, workers' locations are not always processed locally, but are sent to a central server instead.

One more common scenario element is automatic payment of road tolls and other travel fees, as well as automatic payment for purchases. This implies that credit card details are stored in a personal device and transmitted during the payment process. Other personal financial data, such as income, are also known to AmI systems in work and home environments.

Intimate and sensitive data such as health information are also often stored either locally on a smart card or another personal/wearable device – which can get lost or stolen – or in a central (or distributed) database which may not be sufficiently secured and, even if it is, data can be misappropriated by malicious employees. Moreover, since health information is needed in more than one place, a large amount of data transmission is associated with health applications. This includes the regular transmission of new data from sensors to possible central databases, but also extensive ad hoc communication. During this ad hoc communication, the most sensitive information (identity, health history, etc.) is exchanged. It is also worth noting that health data can be acquired not only during health monitoring, but also during evaluation of a person's feedback by physiological sensors (as suggested in Oresteia project scenarios and affective computing), and in such cases, the data might not be protected at all.

Less sensitive data, but also of high interest to diverse organisations and different people (to shops for personalised advertisements, to employers, to terrorists or religious sects for recruiting new members, to insurance companies, etc), are collected for personalisation purposes, stored either on a personal device or in a central database (e.g., customers’ data

are often stored in a retailer's database) and often exchanged for providing personalised services.

Information flow is usually asymmetric between customers and service providers: customers transmit their (sensitive) personal information to the AmI shopping and commerce system while the system provides mainly unproblematic (mass) data including product and price information.

To summarise, since the boundaries between different environments get blurred (people work and buy things from home and on the move, make doctor's appointments and check children from work) and since continuous monitoring (which includes storage of data) of a person's health and actions becomes common, all kinds of information about the person can be acquired anywhere.

# 5 ENABLING TECHNOLOGIES

In this section, we present the most frequently mentioned technologies that enable AmI services together with a critical examination of associated threats posed by and vulnerabilities in such technologies.

## 5.1 UBIQUITOUS COMPUTING

A common vision of ubiquitous computing is that computers will be everywhere, invisibly integrated into everyday life and providing proactive support to people in their diverse activities. The main components of this vision are:

- highly reliable hardware with long-lasting power supplies and of different sizes, from smart dust to huge public screens;
- pervasive wireless communications between computers;
- intuitive interfaces which everybody can easily use, e.g., a natural speech interface;
- embedded intelligence capable of controlling interfaces and communications, self-configuring and self-repairing, reasoning about people and the world around us and doing all this unobtrusively.

Inevitably, this vision implies enormously increased autonomy of computers, both in the sense that computers will need less (direct) user input than today and in the sense that users should not care about what's going on inside computers. From the privacy point of view, hardware as such is of less interest than other components of the vision. The main privacy threats presented by hardware are: first, the smaller intelligent devices become, the harder it is for people to even notice them, let alone remember that they are observing us.

Second, it is easier to lose (or steal) a small smart personal belonging than a notebook or a laptop. It is easier to steal a mobile phone than a suitcase, but the growing amount of data stored in small phones makes them more valuable than suitcases. In the near future, even toys will store a lot of information about their owners, and toys can be lost or stolen even more easily than phones.

Ubiquitous computing systems cannot function without collecting data about the users, and this accumulation of personal information is already threatening privacy. However, the main privacy threat is caused by the possibility to link data about the user accumulated in different parts of the system. To minimise this danger, it is proposed that the users' identities should be hidden as much as possible, and interactions with different subsystems should happen under pseudonyms or anonymously.

Essentially, threats arising from the pervasiveness of ubiquitous computing depend on several things:

- first, what kind of information about people is stored;
- second, what kind of information is transmitted between system components;
- third, what kind of information is presented by the system to people;
- and last, how long-term usage of AmI and growing dependability on it affects humans.

All these issues need to be taken into account in future technology development, and safeguards should be built into enabling technology from the beginning rather than adding it later as an afterthought.

## 5.2 UBIQUITOUS COMMUNICATIONS

Almost all scenarios require ubiquitous communications, and it will be mainly wireless communications connecting literally everything: people (more precisely their personal devices), pets, objects (cameras in parking lots, food products, clothes, home appliances, cars, passports, wallets and so on endlessly) and organisations (e.g., hospital, city administration, bank, border control system). Moreover, it is assumed that wireless connections can be established everywhere and maintained seamlessly on the move with sufficient bandwidth to provide fast access to large quantities of data and fine-resolution images and videos, and that high density of communicating nodes is not a problem.

This vision requires interoperability between all kinds of short-range and long-range wireless and wired networks (body area networks, personal area networks, virtual home environment, ad-hoc, cellular, sensor, satellite networks, etc) and their convergence into all-IP all over the world.[96] Ubiquitous communications present challenging problems from the point of view of privacy protection.

Privacy can be protected:

- first, by reducing the amount of transmitted personal data (it is the task of embedded intelligence to process as much personal data as possible in the personal device and to decide which data to transmit);
- second, by encrypting the transmitted data; and
- third, by designing the system in such a way that all parts are secure. Security expert Bruce Schneier states that cryptography is not magic security dust and that "Security is not a product, but a process." and has cited impressive examples of broken cryptographic algorithms. [97]

At least the first two approaches are already widely accepted as required functionalities, and researchers work actively on their implementation. However, this is protection at the application level, but protection should start from the lowest network levels such as communication protocols, and current communication protocols are rather more concerned with efficiency of data delivery than with privacy protection. Moreover, privacy and security are sometimes contradictory requirements. For example, the report of the Wireless Security Center of Excellence[98] recommends that security of GPRS networks (used currently for Internet access by mobile phones) be strengthened by storing device logs, which is a risk for privacy.

Essentially, communications between people and organisations fall into two major categories: first, communications which require the ability to link data to the user identity;

---

[96] Alahuhta, P., M. Jurvansuu and H. Pentikäinen, "Roadmap for network technologies and service", *Tekes Technology Review* 162/2004, Tekes, Helsinki, 2004.

[97] Schneier, B., "Risks of Relying on Cryptography", in *Communications of the ACM* 42, No. 10, 1999, p. 144.

[98] Whitehouse, O., *GPRS Wireless Security: Not Ready for Prime Time*, Research report, @Stake, Inc., Boston, 2002. http://www.atstake.com/research/reports/acrobat/atstake_gprs_security.pdf.

second, communications which don't require such linkage. Communications of the first type might require linkage for different reasons, such as billing the right person. Other examples can be a worker who needs to be sure that the task was set by his superior; or if a person sells something via the Web and does not deliver goods after receiving a payment, there should be means to find this person. Thus, in communications of the first type, the main goal is to hide the user's identity from everybody except authorised persons, and currently in many aspects, it is trusted to operators and service providers.

In communications of the second type, the main goal is to hide the user's identity completely. For example, if a person buys something and pays immediately, or simply surfs the Web having paid in advance, this does not present a danger to anybody. Unfortunately, due to using unique identifiers in communication protocols (IP addresses, MAC addresses, Bluetooth physical device ID, UIDs of RFID tags, IMEI code of mobile phones), tracking of communication links between devices is relatively easy, and this raises a question about whether pseudonymity and anonymity are achievable at all. In the case of mobile phones, unique identifiers allow tracking of personal location not only by GSM cell, but also by point of IP access and Bluetooth communication.

Communications between objects is also a very popular element of AmI visions. Currently, the main enabling technology is RFID tags embedded into objects. RFID tags don't need batteries and are small enough to be embedded into objects of all kinds, making computing truly ubiquitous.

Since the primary purpose of RFID technology is inexpensive and automated identification, current RFID communication protocols present very high threats to privacy. In low-cost tags (those which are most likely to be embedded into personal belongings), communication between reader and tag is unprotected, that is, tags send their UIDs without further security verification when they are powered from a reader.[99] Thus, tracking a person by reading the UID of his eye-glasses, keys or wallet becomes possible. Second, even those high-end ISO 14443 tags which provide access control to the memory (currently ISO 14443 is used in Malaysian second generation e-passports (Juels 2005)) still use UIDs in collision avoidance protocols. Thus, if once a passport's UID was associated with a user's identity (e.g., the user was recognised by face), then the next time the user shows the passport he will be recognised by the passport's UID without need to read the protected memory of an RFID tag.

Ubiquitous communication as an enabling technology requires not only universal coverage with high bandwidth, scalability for high density of communicating nodes and seamless connections between different networks, but also privacy-preserving mechanisms on all communication layers.

## 5.3 USER-FRIENDLY INTERFACES

AmI scenarios describe highly advanced user-friendly interfaces, the most popular of which are speech interfaces capable of understanding a person's natural speech (that is, users are not restricted to a set of commands and can use any words and phrases when

[99] Knospe, H., and H. Pohl, "RFID Security", in *Information Security Technical Report* 9, No. 4, 2004, S. 30-41.

talking to an AmI system) and video interfaces capable of understanding and presentation of three-dimensional pictures, including tracking of users' movements. Note that there might be many people moving and talking to an AmI system, and the system should be capable of understanding who has done or said something. Recognition of users' emotions by voice processing, image processing or physiological measurements is also often mentioned in scenarios. Privacy threats here depend on the context of the interface, on what the system is doing with the user data and whether the interface is to a public or personal device.

Interaction with large public screens is often mentioned in scenarios as a way to increase user convenience. Public screens present privacy threats because the users do not have any control over the logging of their interactions with a public device. Thus, public interfaces should have built-in capabilities to hide user interactions from everybody but authorised persons.

## 5.4 EMBEDDED INTELLIGENCE

An incomplete list of embedded intelligence functions[100] includes context recognition, data mining, pattern recognition, decision-making, information fusion, personalisation, adaptivity, ontologies and security.

The term "embedded intelligence" denotes the system's capabilities to infer the user's context from whatever input is available and to reason about how to use data about the inferred context: in proactive suggestions to the user or in acting autonomously on the user's behalf. For doing this, embedded intelligence needs to learn about the user's personality from observations of the user's behaviour, and to store the acquired data for future use. Storage of personal data presents privacy risks in cases when these data can be accessed, either when the device is with the owner or not (it could be lost or stolen). Privacy protection in this case is closely linked to security, but security alone is not sufficient.

Since it is improbable that users will devote significant effort to control a flow of their personal data, it should be the task of embedded intelligence to select which privacy policy is appropriate in a particular context and to minimise storage and transmission of personal data. For example, of many possible data mining algorithms, the ones which store selected features should be preferred over those which store raw data. Fule has proposed that sensitive patterns in data mining be detected automatically and treated cautiously.[101]

Current security mechanisms are mainly concerned with protection of personal data during transmission (e.g., by encryption), from being intercepted when the device is with the owner (by not allowing execution of external untrusted code) and with protection of the personal device from being switched on by someone other than the owner (authentication by PIN codes, passwords and biometrics is currently done only when the user logs in). Apart from the fact that "password crackers can now break anything that you can

[100] By "embedded intelligence", we mean the part of ambient intelligence which performs reasoning.

[101] Fule, P., and J.F. Roddick, "Detecting Privacy and Ethical Sensitivity in Data Mining Results" in V. Estivill-Castro (ed.), *Computer Science 2004*, Twenty-Seveth Australasian Computer Science Conference (ACSC2004), Dunedin, New Zealand, January 2004, Australian Computer Society (CRPIT, 26), 2004, pp. 159-166.

reasonably expect a user to memorize"[102], these security measures are not user-friendly, which means that they are used more or less randomly. Indeed, how often does a user in practice enter a PIN code or touch a fingerprint sensor?

Personal devices are often lost or stolen in an "on" state (after the owner has logged on) when personal data are not protected. Thus, in addition to the need to improve existing security methods, new security mechanisms which perform continuous recognition of the owner should be developed, and possibly personal data should be stored encrypted.

With the increased autonomy of computer devices of all kinds, the security of contents residing there becomes a major issue. One of the main tasks of embedded intelligence in most AmI scenarios is personalisation, which to a great extent means filtering incoming information according to a user's personal preferences and capabilities. However, since current security mechanisms are mainly directed against theft of personal data, they don't really check how trustworthy incoming data are. This allows manipulation of contents received by the user. Another example of how acceptance of untrustworthy incoming data can cause harm is phishing. To prevent phishing, security mechanisms are needed to check the legitimacy of incoming data.

The last but not least task of embedded intelligence is providing a user with a means to understand its functions, and to switch them off easily if the user dislikes something.

## 5.5 SENSORS AND ACTUATORS

The most common sensors mentioned in AmI scenarios are positioning, biometric authentication, physiological and health condition sensors. The most popular position determination technology outdoors is satellite-based, such as that provided by the Global Positioning System. The most popular position determination technologies indoors are ultrasound-based, WLAN-based and RFID tag-based. Privacy threats in these technologies depend on where the position is actually calculated, in the personal device or in the infrastructure, and on use of unique identifiers of people or objects inside the system. Further development of positioning technology requires an increase in positioning precision and wider coverage. Currently, GPS does not work well in so-called urban canyons. It requires applications that do not disclose users' locations to third parties, but this is the task of embedded intelligence.

Biometrics as an enabling technology are not mature yet. The main privacy concern in biometric applications is prevention of identity theft. One important direction of development is "aliveness" detection – security against spoofing the sensor by artificial biometrics, such as fake fingerprints. Another important direction of development is unobtrusive identification, that is, identification which does not require an active effort on the part of the user and which can be performed continuously. Currently, unobtrusive biometrics (such as face, voice and gait recognition) are not reliable enough, while using reliable biometrics (such as fingerprint or iris recognition) is time-consuming. Another important research problem is storage of biometric data in such a way that they cannot be stolen, for example, in the form of encrypted templates which would prevent restoration of

[102] Schneier, B., "Customers, Passwords, and Web Sites", in *IEEE Security & Privacy Magazine* 2, No. 5, 2004, p. 88.

raw data. Yet another problem is interoperability between different biometrics systems, which means standards are needed for biometric data storage and exchange.

Physiological sensors in AmI scenarios are suggested for the purpose of recognising user emotions, but we think that they could easily violate privacy in the sense that people often hide their emotions behind neutral or fake facial expressions. Thus, revealing a person's true emotions even to a computer could be dangerous, since data protection is not perfect yet and won't be in the near future.

Sensors for evaluating health conditions are envisioned to be tiny and very sophisticated (the so-called "lab on a chip" capable of performing various physiological tests), and often capable of continuous monitoring and detection of anomalies, including life-threatening ones such as heart attacks. Another group of sensors often mentioned in the scenarios with decisive impacts on people's lives are sensors used for driving safety, and they are rarely named explicitly. Apart from precise positioning, these sensors detect obstacles, estimate road conditions, sliding and grip.

Actuators in AmI scenarios are assumed to function invisibly in the background, switching on and off diverse home and office appliances, health maintenance systems, transportation systems (e.g. taking care of driving safety) and access control systems, and there needs to be plenty of them, all reliable and invisible. They can have a power over people's lives in cases when they give medicines or control cars. Personal identification sensors and health-related sensors and actuators are often envisioned as implants.

## 5.6 DEALING WITH THE WEAKNESSES IN ENABLING TECHNOLOGY

To make technology more protective of privacy, researchers need to develop communication protocols which take care of privacy not only at the application level, but also at lower levels, and which avoid use of unique identifiers in all cases, especially those where the user's real identity is not needed. Researchers also need to develop effective and inexpensive ways to control reading of RFID tags, and not only their memory, but also their IDs. They also need to develop methods for protecting data held on personal devices and embedded in everyday objects in a user-friendly continuous way, unlike current practices which are not so reliable and not so user-friendly (e.g., supplying passwords only at the moment of switching a device on). Also needed are methods of checking how trustworthy is a source of incoming data (currently mainly executable files are checked, not advertisements). There is also a need for algorithms that can detect sensitive data and minimise the amount of stored and transmitted sensitive data.

Our main conclusion from our analysis of current technologies is that privacy protection requirements are somewhat contradictory to the requirements for low cost, high performance and intelligent reasoning, and even to security requirements. Thus, unless privacy protection is built into AmI systems as one more design requirement, users themselves would not be able to do much or enough to protect their personal data, especially in view of the fact that many people are simply too lazy or don't know what they can do to protect themselves, or unable to cope with the technology.

# 6 EXISTING LEGAL FRAMEWORK FOR AMI

Article 8 of the **European Convention of Human Rights** (ECHR) can be considered as the source for EU legislation dealing with privacy and the protection of personal data. Although many of the problems in AmI relate to data protection, the use of invasive technologies might be evaluated from the point of view of privacy such as protected by article 8 ECHR. The two most important European instruments concerning data protection are the **Data Protection Directive** 95/46 and the **Privacy & Electronic Communications Directive** 2002/58. The problems and challenges of data protection law in relation to AmI mainly concern the reconciliation of the principles of data protection law with the concept of AmI. This means that not only should concepts, scenarios, practices and techniques of AmI be tested for their compliance with data protection law; also data protection law itself can and should be put into question if necessary, e.g., where some data protection rights can not be reasonably reconciled with good practices and techniques of AmI that are desired by the user. An important document in the field of data protection and international co-operation is the **Safe Harbour agreement** concluded between the U.S.A. and the European Union.

When discussing e-commerce and **consumer protection law**, Directive 93/13 on unfair terms in consumer contracts is pertinent. Since AmI users will become increasingly dependent on services there is a significant risk that the suppliers of AmI services will acquire more power and will abuse it. Directive 97/7 on consumer protection in respect of distance contracts determines which information should be provided to the consumer in this context. Since its provisions are not fitted for the environment of modern mass communication, this obligation might encounter certain problems in an AmI world. The e-commerce directive 2000/31 sets out rules concerning unsolicited commercial communications and the liability of the intermediary service provider in case of mere conduit, caching and hosting. In an AmI world, spam and unsolicited communications will become an even bigger problem than they are today and this directive tries to protect consumers from it. The opt-out registers, however, seem to be insufficient and impractical.

Directive 85/374 on **liability for defective products** stipulates that producers are jointly and severally liable. It also creates a "liability without fault" (or strict liability) because it is "the sole means of adequately solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production." The directive does, however, not apply to services and it is unclear whether it applies to software.

Directive 91/250 harmonises the **copyright protection** of software within the European Union. The exceptions foreseen to allow the use of computer programs without prior authorisation seem to be insufficient to allow the free use of computer programs required in an AmI world. Directive 96/9 harmonises the legal protection of databases. This is important for AmI because most scenarios require the linking and integration of several databases for providing AmI services. The exceptions provided to the exclusive right of the maker of the database are rather limited and optional, which could hamper the creation and delivery of AmI services. Finally the Copyright Directive 2001/29 harmonises copyright protection in the European Union in several important aspects and reassesses the exceptions to the exclusive rights of the right holder in the light of the new electronic environment.

Directive 1999/93 creates a legal framework for **electronic signatures** and for certain certification services. They might facilitate the use of pseudonyms on the Internet and enhance the security of electronic transactions in an AmI world. The directive's obligation to publish generally recognised standards might solve problems of interoperability. Another important legal document concerning standards is directive 98/34/EC on technical standards and technical regulations in Information Society Services, which foresees a detailed information and co-operation procedure. Directive 90/385 on active implantable medical devices sets out strict essential requirements which have to be fulfilled by implantable medical devices in order to ensure a high level of safety. In an AmI world, implants will be used for non-medical reasons and this might require even stricter rules.

Directive 98/84 on the protection of services based on conditional access is important, since many services in an AmI world will rely on conditional access. The **Cybercrime Convention** of 23 November 2001 obliges the Parties to create the necessary substantive legislation and other measures to for a number of criminal (cyber) offences. The AmI world will be one without borders and thus it is important that all countries define criminal offences in a similar way. While the Convention is a good initiative, its utility so far is limited by the fact that so few countries have ratified it.

The Convention of Rome on the Law Applicable to Contractual Obligations contains rules on the applicable law in case of cross-border legal issues. An important question is which law is applicable when the ambient intelligence service is delivered in one state, the contract made in another state and the data are collected in a third state. Some rules on which (data protection) law is applicable can be found in the relevant data protection legislation. The applicability of the national law of the data subject (personae criterium) instead of the place of the processing (territory criterium) should be put into question. Regulation 44/2001 on jurisdiction and enforcement aims to unify the rules of conflict of jurisdiction in civil and commercial matters, and in the case of consumer contracts concluded via new means of communication.

The **anti-discrimination** principle is well established in European law. It has its place in Treaties (Article 6 of TEU, Articles 2, 3, 12, 13 of TEC), international Conventions (European Convention for the Protection of Human Rights and Fundamental Freedoms and Protocol No 12 to the Convention), the Charter of Fundamental Rights of the European Union and a wide range of secondary Community legislation. The general principle of non-discrimination will apply also to decisions taken in the AmI environment, and may fill gaps in the legal provisions of specific instruments such as data protection law. So far, however, there has not been much attention given to the applicability or adequacy of anti-discrimination provision in the context of new technologies.

Consideration should be given to the extent to which there might be a need to provide certain emerging AmI services to all individuals. The **Universal Service Directive** 2002/22 recognises the need to provide certain "universal services" to end users at affordable prices, but its scope is limited to only electronic communication networks and certain services.

In conclusion, there are a number of legal instruments that could serve as safeguards in a world of ambient intelligence. However, their utility as safeguards is not a sufficient solution since there are various lacunae which would need to be remedied, not least of which is their limitation to Europe.

# 7 DARK SCENARIOS

Since its conception, the AmI vision has been taken up and refined by different actors and institutions. A range of scenarios has been developed to depict the different futures of living and working with AmI. Scenarios are considered as one of the main tools for looking at the future, although there are many other prospective methods such as Delphi expert panels. Scenarios are not predictions. Rather, they describe plausible and/or desirable futures and possible ways on how to realise these futures. The objective of many scenario exercises and foresight studies is to present images of *desirable* futures. Consequently, they have an inherent bias towards presenting only optimistic visions of the future.

The scenarios developed by SWAMI provide provocative glimpses of potential futures and were developed to stimulate debate, but unlike most other scenario exercises, our scenarios present visions of the future that we do NOT want to become realities. SWAMI has labelled them "dark" scenarios.

They do not depict extreme, impossible or unlikely futures. They are not anti-technology or neo-luddite, i.e., categorically opposed to technologies in general and to AmI in particular. On the contrary, the SWAMI dark scenarios are intended to be constructive towards realising AmI. Their objective is to highlight potential risks that need to be mitigated if AmI is to become a success. As such, the dark scenarios are intended to alert policy-makers and AmI developers and designers to the need to develop safeguards to minimise the risks that could emerge in this new intelligent environment.

## 7.1 THE SWAMI DARK SCENARIOS

### 7.1.1 Methodology

From a methodological point of view, the SWAMI scenarios are so-called trend or reference scenarios, i.e., extrapolations from current trends.[103] They start from the present and work forward to realistic futures. As there is no unique method for developing scenarios (i.e., there are different approaches to scenario-writing), it is important to clarify and explain the approach and methodology used by SWAMI.[104]

From the outset, SWAMI decided to develop a number of dark scenarios typical of many scenario exercises, namely four. In principle, a virtually infinite number of possible futures could be developed but it is difficult to manage for both the developers and the readers of

[103] Massini, E.H. & J. M. Vasquez, "Scenarios as seen from a human and social perspective", *Technological Forecasting and Social Change*, 65, 2000, pp.49-66.

[104] For an overview of foresight methodologies for the knowledge society, see Miles, I., M. Keenan and J. Kaivo-Oja, "Handbook of Knowledge Society Foresight", European Foundation for the Improvement of Living and Working Conditions, Dublin, 2003. This handbook is available in electronic format only: www.eurofound.eu.int.

the scenarios.[105] Moreover, the design of four scenarios in a scenario exercise makes it possible to plot them on two axes and four quadrants.[106]

The SWAMI scenarios were developed through a combination of desk research and interactive workshops within the consortium and with outside experts in keeping with the view that scenarios should not be based on only desk research.[107] More specifically, the SWAMI dark scenarios were constructed as a result of the following activities:

- a state-of-the-art review of projects, studies and scenarios on ambient intelligence, including an investigation of the current legal framework in Europe, as reported in SWAMI Deliverable 1;[108]
- a full-day workshop (1 June 2005) with 13 external experts to brainstorm on the major drivers and axes for developing dark scenarios;[109]
- an internal working document summarising the dark scenario brainstorming discussion;
- an internal two-day consortium meeting (28-29 June 2005) to discuss and develop the basics of the scenario scripts and scenario analysis;
- further development of the scenarios and their analyses via electronic exchanges between the partners;
- a workshop with 15 external experts to validate the draft report of the scenarios including their analyses and to develop safeguards (29 November 2005).

The SWAMI scenarios assume a wide deployment and availability of ambient intelligence based on the ISTAG AmI vision of a future information society where intelligent interfaces enable people and devices to interact with each other and with the environment. Technology operates in the background while computing capabilities are everywhere, connected and always available. AmI is based on the convergence of ubiquitous computing, ubiquitous communication and intelligent, user-friendly interfaces. This intelligent environment is aware of human presence and preferences, takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire. It can even engage in intelligent dialogue. It is about "human-centred computing", user-friendliness, user empowerment and the support of human interaction.

The SWAMI partners decided to develop four scenarios that highlight potential threats and vulnerabilities in a way that is relatively easy to read and digest. As a result, the scenario stories are not an end in themselves. SWAMI scenarios contain a "technology check", i.e., references to RTD projects and publications that are, for example, trying to provide solutions to the mentioned problems or that may raise important vulnerabilities. This is also the case for the "reality check", i.e., the references to recent news reports (especially)

---

[105] Godet, M., "The art of scenario and strategic planning: tools and pitfalls", *Technological Forecasting and Social Change*, 65, 2000, pp.3-22; Gavigan, J.P., F. Scapolo, M. Keenan, I. Miles, F. Farhi, D. Lecoq, M. Capriati, T. Di Bartolomeo, (eds.), "A practical guide to Regional Foresight", EUR 20128 EN, IPTS, Sevilla, December 2001.; Wilkinson, L., "How to Build Scenarios", *Wired* 3, Special Issue. http://www.wired.com/wired/scenarios/build.html

[106] In the IPTS/ISTAG scenarios on ambient intelligence, for instance, the two axes are efficiency versus sociability and individual versus communal. They contrast applications that serve to optimise efficiency (whether in business or in society) against those that emphasise human relationships, sociability or just having 'fun'. They also underline the place of ambient intelligence in serving society and the community as well as individuals. See ISTAG, 2001.

[107] Godet, M., 2000, p.17.

[108] Friedewald, M., E. Vildjiounaite & D. Wright, 2005.

[109] See WP1 Workshop minutes including the agenda and list of participants on the SWAMI website: http://swami.jrc.es/pages/state_of_art.htm.

of events or situations not so different from those in the scenarios point to the fact that the dark situations are credible and based on reality.

Equally important as the scenario stories is the scenario analysis. SWAMI has developed the following structure for presenting the analysis of each of the four scenarios:

- a short summary of the major dark *situations* mentioned in the scenario story;
- a list of the most important *AmI technologies and/or devices* used and/or implied in the scenarios. These are pieces of hardware or software, such as 4G mobile networks that enable applications to be offered;
- a list of major AmI *applications* that emerge in each scenario. Applications allow certain things to be done with the technologies and devices;
- the *drivers* that have led to the scenarios and/or their (dark) situations. Drivers drive or impel a situation or the scenario. An example of a driver is the individual and/or social wish for privacy or security;
- a discussion of the major *issues* in terms of privacy, security, identity and vulnerabilities raised by the scenario, which are the core concerns of the SWAMI project;
- the *legal aspects* implicit in the scenarios;
- preliminary *conclusions*.

The SWAMI dark scenario approach is summarised in the following graph:

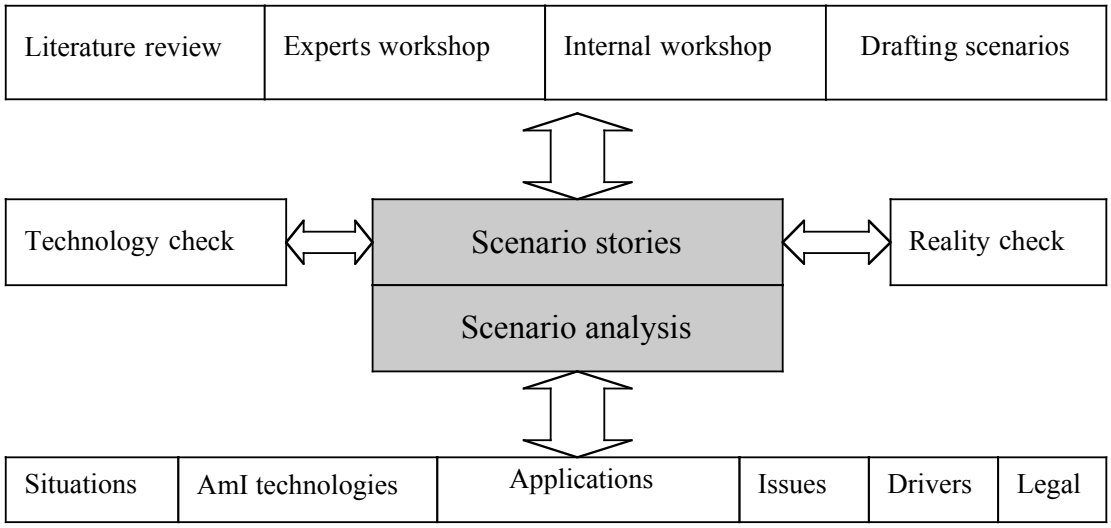


*Figure 3: SWAMI dark scenario approach*

### 7.1.2 Drivers and issues

The choice to develop certain scenarios and not others is based on the methodology mentioned above. It is certainly not arbitrary. Scenario workshops were used to identify the most important drivers that gave rise to the kind of scenarios being developed and to identify the most important issues that needed to be present in the scenarios.

### 7.1.3 The four scenarios

SWAMI developed four scenarios as follows:

- Dark scenario 1: A typical family in different environments – presents AmI vulnerabilities in the life of a family moving through different environments. It introduces dark situations in the smart home, at work and during a lunch break.
- Dark scenario 2: Seniors on a journey – also references a family but focuses on senior citizens on a bus tour. An exploited vulnerability in the traffic system causes an accident and raises different issues related to both travel and health AmI systems.
- Dark scenario 3: Corporate boardroom & court case – involves a data-aggregating company that becomes victim of theft of the personal data that fuel its core business. Given its dominant position in the market, the company wants to cover this up but will face the courtroom two years later.[110]
- Dark scenario 4: Risk society – portrays AmI from the studios of a morning news programme. It presents an action group against personalised profiling; the digital divide at a global scale and related to environmental concerns; the possible vulnerabilities of AmI traffic systems and crowd management in an AmI environment.

The first two scenarios depict the impact of AmI dark situations on the individual and the family in their everyday life. The impact of the AmI dark situations on the individual is at the micro-level. In scenarios 3 and 4, the impact is on a larger societal scale. The theft of personal data in scenario 3 affects millions of people. Scenario 4 also depicts the societal impact of AmI technologies on privacy, the environment and crowd behaviour.

In addition to the individual-societal axis, we have drawn a public-private axis for positioning the scenarios. Scenarios 1 and 3 deal with private concerns and/or with what might be called the private sphere. Scenarios 2 and 4 encompass concerns situated in the public sphere. Scenario 3 draws out concerns in the transport and health sectors which are regulated by public actors while scenario 4 draws out other public concerns, including those relating to the environment. The combination of the axes individual/societal and private/public enables each scenario to be placed in a different quadrant.

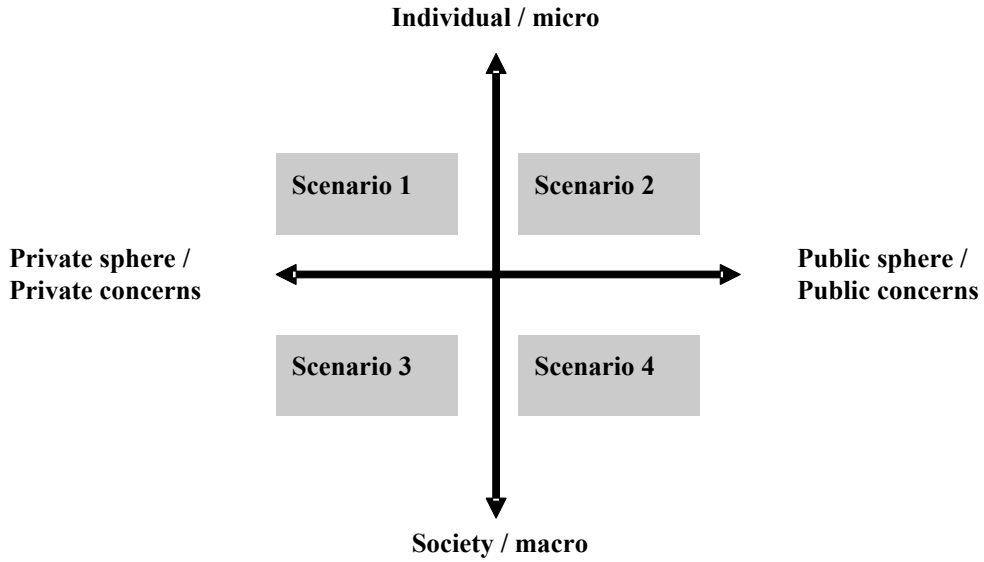


*Figure 4: Positioning of the four dark scenarios*

[110] This third scenario, together with analytic methodology used for deconstructing it, can be found in Wright, David, et al, "The illusion of security", *Communications of the ACM*, forthcoming (2007).

Thus, as shown in Figure 4, the four scenarios address individual and societal concerns as well as private and public concerns. Nevertheless, the scenarios are constructed from the point of view of the individual citizen, in part to indicate that also societal concerns are experienced by people in their everyday life, be it at work, at home or on holiday or via a TV newscast. Grounding the scenarios in everyday life helps us to reflect upon the use of AmI in situations with which we can identify today and in the future.

# 8 AN EXAMPLE OF A DARK SCENARIO: SENIORS ON A JOURNEY

In this chapter, we present one of the four scenarios developed by the SWAMI partners, as an example of a dark scenario and to show how dark scenarios can be deconstructed and analysed.

## 8.1 THE SCENARIO SCRIPT

### *8.1.1.1 Introduction*

As a former software engineer, Martin Schmitt, born 1943 (aged 77 in 2020), is familiar with technology. His wife Barbara is 75. The Schmitts have lived for more than 10 years in a village in the alpine upland that has been specifically designed for senior citizens and is equipped with ambient intelligence technology. For their age, they are both healthy. The Schmitts' daughter Heike has her own family now and they live in northern Germany. Heike sees her parents only once or twice a year, but maintains contact during the rest of the year by means of AmI. The Schmitts are on a tour for senior citizens to Florence.

### 8.1.1.2 *Scene 1: News from the police report: Senior citizen dies after bus accident*

Florence – Twenty-four senior citizens were injured in a bus accident Friday afternoon. An 84 year-old woman died under tragic circumstances. According to Florence police reports, the bus was on a sightseeing trip with 46 senior tourists from Germany and Austria when, for unknown reasons, the traffic lights at a major intersection went to green for all directions. The bus driver avoided a collision with the oncoming traffic but knocked down some traffic signs, went off the street and finally crashed into a lamppost.

Fifteen of the passengers on the bus had minor injuries and were released from the hospital shortly after. Nine were more seriously injured and had to be treated at the Careggi Hospital. Though the emergency service arrived quickly, the severe internal injuries of an 84-year-old woman from Austria remained undetected because she used an outdated health monitoring system. She died on the way to the hospital.

*Automated alarm messages from HMDs*

*Heike Lengbacher-Schmitt is sitting in the subway on her way home when she suddenly receives two alarm messages on her personal wrist communicator (PWC). Her parents' health monitoring devices (HMD) issued the alarms, indicating that a critical situation had occurred.*

*Of course, Heike becomes concerned. She had picked up similar messages before from one of her parent's HMD, and in all of these instances things eventually turned out to be fine. But this was the first time she received alarms from both parents at once. Moreover, she knows that her parents are on a bus tour, making the situation even more worrisome.*

*No direct contact*

*Heike's attempts to call her parents are not successful. As she learned later that day, in an emergency situation, the HMDs by default block any incoming communications from people not directly involved in the*

*rescue efforts in order not to disrupt the immediate rescue process. And during the examinations at the hospital, mobile communication devices are required to be turned off.*

*Over the course of the next three hours, she leaves numerous messages at her parents' digital communication manager, urging her parents to return her calls as soon as possible.*

*Superfluous, decontextualised information*

*In addition, Heike accesses her father's personal data storage. The system recognises her and, because she was granted comprehensive access rights beforehand, releases large amounts of information such as geographic locations, stopovers, local temperatures, etc. All of the impersonal and unspecified information raises even more questions, however, making it very difficult to grasp her parents' situation. Heike is not really relieved by the data, on the contrary. At least, she eventually finds out that her parents are at the Careggi Hospital in Florence. After phoning the Hospital, Heike is informed that her parents are receiving medical treatment.*

*After Martin Schmitt has been thoroughly examined, he is allowed to leave the emergency room and turn on his communication devices again.*[111] *He immediately calls his daughter.*

*Phone call*

*Heike: Hello? Oh, it's you, dad. Thank goodness! Are you all right? How's mom? What happened?*

*Martin: Don't worry honey, we're fine. Our bus had an accident, and your mom was slightly injured, nothing serious. She has a slight concussion and I have a few scratches. Nothing to worry about, believe me.*

*Heike: Can I talk to her?*

*Martin: Sorry honey, but she's still being treated and the doctors said she should not be disturbed.*

*Well meant services act against the user's will and may have rebound effects…*

*Heike: By the way, Aunt Anna called me just a few minutes ago. She was totally freaking out because she received the same alarm messages as I did. Apparently she became so excited that her HMD even alarmed her doctor!*

*Martin: Oh no, I forgot to take Anna off the list of people to be automatically notified in an emergency. Please call her for me and try to calm her down. Listen, I want to go back to your mother. I'll call you later. Just wanted to let you know everything's okay.*

*Heike: Tell mom we're with her. And don't forget to call me; I have to*

[111] At the moment it is debated if wireless technology can be banned from hospital any longer or if "wireless tagging is 'inevitable'". Carr, S., "Wireless tagging in hospitals is 'inevitable': Prepare to be chipped...", silicon.com, 7 December 2004. http://hardware.silicon.com/storage/0,39024649,39126387,00.htm

*know what happened!*

*Video messages*

*As it is already past midnight when Martin finally leaves the hospital, he decides to send a video message to his daughter instead of calling her. In his hotel room, Martin sets up his mobile phone in front of him and starts recording his message. He also attaches a short clip showing Barbara in the hospital, saying a few words to reassure her daughter. Martin had ignored the ban on using mobile recording devices in the hospitals and filmed a short video-sequence of his wife anyway.*

*Dear Heike! As you can see, I'm absolutely fine. And your mother is recovering quickly. She will be released tomorrow morning. But let me tell you what happened from the beginning.*

#### *8.1.1.3 Scene 2: Travel preparation and check-in procedure for public transportation*

*Travel preparation*

*Unlike our normal habit, Mom and I actually had completed travel preparations way ahead of time. So there was no need to get stressed out. And thanks to the travel-assistance procedure of the AmI environment in our home in Murnau, this time we even thought of recharging our PWCs and HMDs early enough to avoid losing "our identity" like on our last trip.*

*Disclosure of location information violates privacy and results in embarrassing situation*

*In Munich, I experienced an awkward situation after I located a former colleague of mine using the "friend-locator" function (LBS) of my PWC.*[112] *I just wanted to say "hi", but when I walked up to him, I was surprised to see that he had a good-looking, younger woman with him who obviously was not his wife. He blushed, mumbled a few words and disappeared in the crowd. It seems difficult to keep secrets these days...*

*Boarding the bus*

*At Munich station, we met our old friends Brigitte and Peter as planned. The four of us proceeded to meet up with the travel group in the new bus terminal, just next to the station.*

*After Alessandra, our Italian tour manager for the next days, had welcomed us to the tour and introduced herself, we finally started to pass through the security gates in order to board the bus.*

*Feeling uneasy - loss of control*

*I guess I'll never feel comfortable with all these safety measures you have to endure when travelling: biometric ID verification,*[113] *detectors for drugs and explosives, etc., especially if they reject you erroneously.*[114]

---

[112] Paciga, M. & H. Lutfiyya, "Herecast: An open infrastructure for location-based services using WiFi, Wireless And Mobile Computing, Networking And Communications", WiMob'2005, IEEE International Conference, pp. 21-28, 2005.

[113] Bolle, R.M., J.H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior, Guide to Biometrics, New York, Springer, 2004.

[114] Maghiros, I., Y. Punie, S. Delaitre. et al., *Biometrics at the Frontiers: Assessing the Impact on Society*, Technical Report EUR 21585 EN, Institute for Prospective Technological Studies (IPTS), Seville, 2005. http://www.jrc.es/home/pages/detail.cfm?prs=1235.

*Denial of transportation*

*Resistance*

*Imagine, one of our fellow travellers, Michael from Baden-Baden, was denied access to the boarding area of the terminal, although he had a valid ticket and even could present the receipt from his travel agent![115] Apparently, some kind of data mismatch between his personal ID, the e-ticket and the information stored on the central server had caused the problem.*

*Legal discrimination*

*The security personnel at the terminal were absolutely stubborn and unwilling to make an exception, despite several interventions by Alessandra and Peter, who, by the way, is a good friend of Michael. The officials urged Alessandra to accept the situation and told her to leave without Michael. But they hadn't reckoned on the solidarity of the whole group – we made it unequivocally clear that we wouldn't leave behind a member of the group. Actually, I was surprised myself that nobody of our party stepped out of line.*

*Imagine. Michael was obliged according to the law to receive a "possible risk status for an unlimited time" because he is causing more security risks than normal. He has to accept this "possible risk status", granted to him by the officer, which means that all his actions and movements are followed and stored, including his presence, actions and movements.*

*Liability*

*To make a long story short, it took about another hour until Alessandra had worked out an agreement with one of the senior officials. The solution was that the tour manager and all passengers had to sign a statement discharging the bus terminal of any responsibility for possible damages caused by Michael. Pretty ridiculous if you ask me, especially considering that once you leave the terminal, anybody can hop on the bus without any security checks at all!*

#### *8.1.1.4 Scene3: Traffic supported by ambient intelligence*

*Mobile entertainment systems*

*After a pleasant stopover in Bolzano, we continued our journey the next day. The ride through Upper Italy was uneventful. Some of us were watching on-demand videos or reading books on their portable screens.[116] And Alessandra turned on the interactive tour guide of the bus that explains what we could see outside the bus if it had not been so foggy in the Po lowland. Instead, some videos of the scenery were projected onto the windowpanes.*

*Traffic jam situation*

*Later on, our bus driver even managed to by-pass a major traffic jam on the highway near Modena. Well, actually he just had to follow the instructions he received on his on-board navigation system. Within seconds after the potential disruption of the traffic flow – later we learned that a severe accident had occurred about 30 km ahead of our position was detected by the traffic monitoring system – a traffic warning and,*

[115] Schneier, B., 2004.
[116] Espiner, T., "Philips unfurls prototype flexible display". http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39216111,00.htm

*almost simultaneously, an alternative route were issued.*

*Cognitive overload avoided*

*Thanks to the intelligent filtering system, our driver was able to take the decision at the right moment without being distracted by too much information while driving.*

*Business model:*

*Luckily, the bus company we were travelling with had subscribed to one of these expensive premium traffic information schemes. Many other people travelling in the same direction weren't as fortunate as we were.*

*Traffic control system*

*In Florence, traffic volume was pretty high, but considering the rush hour, we moved along quite smoothly. The electronic road signs told us that inbound traffic was given priority. In addition, our bus had permission to use the lane reserved for public transport. Paying tolls is always undesirable, but these urban traffic management systems seem to pay off.*

#### *8.1.1.5 Scene 4: Emergency situation*

*Malicious attack against traffic system*[117]

*But then again, the traffic management systems are far from perfect. The accident we were involved in was, as we learned later on, caused by a kid who illegally used software for priority vehicles like ambulances and police cars.* [118]

*All of a sudden, cars coming from the right entered the junction at high speed. In order to avoid a collision, our bus driver pulled to the left and we ran into the central reserve, hitting all kinds of signs and objects. Finally, we crashed into a large lamppost and came to a brutal and sudden stop.*

*(medical) reassurance thanks to AmI*

*It took me a few moments to realise what had happened and to regain orientation. Your Mom was obviously unconscious because she didn't respond to me. So I checked her HMD immediately. The display indicated that an emergency call had already been issued. Thank goodness, all vital parameters such as blood pressure and pulse rate were okay.*

*Selling surveillance pictures/videos to the media*

*I looked around and saw the mess we were in. You should see the camera images taken in the bus (as you know, the cameras in the bus record everything constantly), but they were not immediately available because the bus company gave commercial exclusivity to a television station… So we have to wait until the police give us a copy, if we ever get one.*

*International interoperability,*

*What I did not know was that some passengers were using HMDs that are not compatible with the Italian system. Thus, they were not able to download the health information of a couple of people on the bus and the*

[117] Poulsen, Kevin, "Traffic Hackers Hit Red Light", *Wired News*, 12 August 2005. http://www.wired.com/news/technology/0,1282,68507,00.html

[118] In summer 2005, the US government outlawed the possession of "traffic signal-pre-emption transmitters" after hackers had used them to manipulate traffic lights. Poulsen, K., "Traffic Hackers Hit Red Light", *WiredNews*, 12 August 2005. http://www.wired.com/news/technology/0,1282,68507,00.html.

*semi-automatic rescue co-ordination centre assumed there were only 32 people on board and sent too few ambulances. This did not have severe repercussions since many of us were not seriously hurt.*

*System cannot distinguish reason and effect*

*The police, ambulances and fire brigade arrived rather quickly. The fire brigade, however, was not needed. It was called because the alarm signal stopped after three minutes due to a power shortage in the vehicle and the rescue centre interpreted this as an indication that the bus might have caught fire – the travel organisation will have to pay for this service, but who wants to grouse?*

*AmI divide!*

*On their way, the paramedics had checked the medical records of the passengers and the HMD signals and set up a list of people with more serious injuries and those with private health insurance.*[119] *Apparently, they were given priority treatment and transport to the hospital. Too bad we didn't opt for such insurance and had to wait for more than half an hour before being examined.*[120]

*Exchange of identity*

*A "funny" incident happened when my neighbour was almost given an injection just because he had not picked up his own but someone else's HMD.*

*Service quality and system update or even opt out*

*Delegation human decision to technology*

*But something really tragic occurred with Monika Klein, a nice 84-year-old lady from Salzburg. She was one of those whose health insurance refused to pay for an update of the HMD to the latest model; and the paramedics had neither her patient record nor her current vital data. When one of the paramedics walked around and talked to those who were not on his automatically-produced list, she told him that she was not in pain, only exhausted. Because there weren't enough ambulances at the scene, they left her sitting on a bench next to the road. Since the introduction of HMDs, these guys depend too much on the technology. They are not even able to practise the simplest diagnosis. Otherwise they would have diagnosed that Mrs Klein had internal bleeding. I heard that when they finally decided to take her to the hospital, one of the last to go, she suddenly lost consciousness and passed away before the ambulance reached the hospital.*

#### *8.1.1.6 Scene 5: Ambient intelligence and medical care*

*Pressure to disclose personal data*

*After we arrived at the hospital, I had a fierce argument with the lady at the reception who complained that she was not able to access my health and insurance record completely. The doctors, she said, were unable to help me if I wouldn't disclose my complete data to the hospital.*

*Data leakage –*

*Heike, you probably remember that I had forbidden the health services to*

[119] Michahelles, F., P. Matter, A. Schmidt, B. Schiele, "Applying Wearable Sensors to Avalanche Rescue: First Experiences with a Novel Avalanche Beacon" in *Computers & Graphics* 27, No. 6, 2003, pp. 839-847.
[120] Carr, Sylvia, "Wireless tagging in hospitals is 'inevitable'. Prepare to be chipped...", Silicon.com, 7 December 2004. http://hardware.silicon.com/storage/0,39024649,39126387,00.htm

*illegal trade with personal data may lead to spamming*

*give away certain data because I had been flooded with drug advertisements last year after that scandal with the illegal trading of personal health data. I saw no necessity to give the hospital complete access since I only had some scratches. However, I had to sign a statement that the hospital is not liable for any impairment resulting from their treatment.*

*I really wonder if the benefits of automated health care are really worth this mess. I promise to keep you posted. Say hi to George and hug the kids for us!*

*Bye for now!*

## 8.2 ANALYSIS

### 8.2.1 Situations

The scenario presents three different environments that reveal possible weaknesses related to public or semi-public infrastructures and the trade-off between economically efficient procedures as implemented in AmI services and the variety of individual needs.

Citizens must be able to trust and rely on unfailing operation of these infrastructures – especially for vital functions. Fair access and user-friendliness are needed to prevent an ambient intelligence divide. While equal and fair access is the basic requirement for the possibility to use public utilities, user-friendliness is the core factor for the actual use of AmI services. In this respect, disabled and elderly people have a particular demand.

The first scene depicts communication links between an elderly person and his children living far away.[121] Synchronous and asynchronous communication using text, phone or video from basically any location is assumed to be standard. For both the elderly father and his daughter, these communication possibilities are part of everyday life, including receiving all kinds of information automatically issued by personal agents such as HMDs. In an emergency situation, however, automatic alerts can actually cause more harm than good unless they inform the recipient adequately about the situation.

The second scene shows the preparation of the elderly couple for a short trip. The scenario assumes that elderly people remain active up to an advanced age and are supported by AmI technology in their daily activities, including travel preparations.[122] AmI-enabled services can remind users not to forget important things (like an HMD).

---

[121] As presented in Cabrera Giráldez, M., and C. Rodríguez Casal, "The role of Ambient Intelligence in the Social Integration of the Elderly" in G. Riva, G., F. Vatalaro, et al. (eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction*, IOS Press (Studies in New Technologies and Practices in Communication, 6), Amsterdam, 2005, pp. 265-280.

[122] See, for instance, Cabrera Giráldez and Rodríguez Casal, 2005, and Korhonen, I., P. Aavilainen and A. Särelä, "Application of ubiquitous computing technologies for support of independent living of the elderly in real life settings" in UbiHealth 2003: The 2nd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Seattle, 8 October 2003.

In the aftermath of 9/11 and other terrorist attacks in recent years, boarding public transportation usually involves more or less extensive procedures of identification, control and surveillance. People have to get used to it. The imperfection of technology periodically leads to nuisance and sometimes even to open insubordination when results are *obviously* faulty and authorities deny services. An open issue in this respect is the trade-off between public security and individualism.[123]

The third scene explores the delicate balance between market- and supply-driven approaches to many new mobile services enabled by the availability of personal information in fields that are considered public utilities today. This development may result in a decreasing relevance of free and publicly available services and in a growing disparity between those who can afford the benefit offered by ambient intelligence and those who cannot.

Extrapolating from current developments, we can assume that bus drivers (like other traffic participants) will be supported by numerous AmI applications to make driving more efficient and less stressful. Avoidance of traffic jams will undoubtedly be a popular application. As some of these services constitute business models, quality and speed of traffic information services differ according to the price consumers are willing to pay.

AmI technology also supports passenger activities, such as individualised entertainment (video, music, interactive games) and edutainment like an electronic tour guide, which gives explanations about the scenery outside (augmented by videos and other multimedia).

AmI technologies will be an important element in the efforts of big cities to cope with high traffic volumes and recurrent congestion. Traffic management systems constantly monitor and manage traffic flows according to predetermined parameters through centrally controlled traffic signs, traffic lights and other electronic means. Certain vehicles such as ambulances, streetcars, buses, taxis, etc., are granted priority rights. Traffic management systems can be deceived, however, by illegal hardware and software.

In the fourth scene, public authorities have established AmI-supported emergency systems with automated information chains from the individual person and vehicle to the emergency services (police, ambulances, hospital).[124] This has become a complex system, since heterogeneous actors and systems have to communicate seamlessly. Given the fast development of technology, different national standards and health systems, this system remains imperfect – services cannot be offered to all citizens in the same way. In addition to the problems associated with operating efficiency, health and emergency services become increasingly differentiated from basic to premium services, creating an "AmI-divide". For whatever reasons (e.g., because they are using older equipment, live in regions without technical coverage, or even have opted out), people who remain outside the system are at risk of not even being provided with the most basic services.

Like other applications, AmI-enabled emergency systems may be driven by market forces creating differences between people who can afford a premium service and those who cannot. While this is already taking place in the existing health insurance system, it is a sensitive issue who is actually driving the development: the insurance companies and

[123] See, for instance, Fujawa, J. M., "Privacy Made Public: Will National Security Be the End of Individualism?", *Computers and Society*, 35, Nr. 2, 2005.
[124] Savidis, A., S. Lalis, A. Karypidis, et al., 2001.

health care suppliers who are under constant pressure to act economically and efficiently or citizens (represented by the government) who set the rules and define boundaries for AmI health care services.

In addition, identities can easily be mixed up if the link between a person and his/her personal device is dissociated (e.g., picking up the wrong HMD).

The fifth scene reveals vulnerabilities like those in the emergency situation. Hospitals ask for a complete disclosure of health information (regardless of the actual treatment) in order to be on the safe side and avoid liability. Again this poses the question about who is in control of the system and who establishes the rules that apply to denial of services.

In order to reduce possible interference with medical procedures and to protect the patients' privacy, all mobile communication devices are required to be turned off within hospitals.

### 8.2.2 AmI technologies and devices

The scenario makes reference to several AmI technologies:

- Sensors and actuators – embedded in the environment and in objects and attached to people, such as an impact sensor for accident detection and body sensors measuring the vital parameters of the elderly (or people with health risks). Other sensors and actuators are as detectors of drugs and explosives, for positioning and biometrics;
- Interfaces – portable screens, augmented reality displays (such as bus windows)
- Intelligent algorithms – for priority-based traffic routing, routing of network traffic in emergency situations, processing of health data in real time, detection of persons with highest health risks or best insurance
- Communications networks – enabling seamless service by heterogeneous devices with/without central control providing greater coverage (especially for emergency communication).
- Health Monitoring Devices (HMDs) – health-related personal intelligent devices, which could be combined with other multi-functional devices such as a Personal Wrist Communicator.

### 8.2.3 AmI applications

Among the AmI-enabled applications referenced in the scenario are the following:

- *Personal communications management*, like that described in ISTAG's "Dimitrios Scenario"[125], controls the communication of the elderly couple based on the context, e.g., it denies communication in the emergency when communication with the authorities has priority and at the hospital where mobile communication devices are not allowed. On the other hand, it proactively sends messages to family members and recognises people close by ("friend locator").
- *Support for elderly people* helps to enable an independent life to an advanced age. This system reminds users about tasks to be done and objects to taken with them. When coupled to a health monitoring system, it also supports a healthy lifestyle.
- *Check-in and security procedures* for public transportation are technically integrated to a large extent, combining access controls with identification procedures (supported by

[125] ISTAG, Scenarios, 2001.

biometrics and central databases) and security protocols. If operating accurately, the system speeds up regular check-in procedures and helps to detect potential security risks.

- *Personal health monitoring* is used to survey vital parameters of people with certain risks such as high blood pressure or diabetes. The collected data can be used either by a physician for routine examination or in an emergency. The personal health monitoring system may be linked to a health insurance database and a communication system.
- *Public traffic management* collects information about the current traffic and give support to road users either collectively or individually. The business models may vary from free public information to pay-per-advice models.
- *Automated emergency alarming* can detect accidents and the urgency of a situation (especially if coupled with the personal health monitoring devices of drivers and passengers). The rapid alarms and automated requests for assistance improve the quality of the medical system and help to reduce traffic casualties.
- In a *seamless medical information system*, all relevant information is collected, including personal medical history (previous illnesses, treatments, medication) as well as up-to-the-moment vital signs and health insurance information.

### 8.2.4 Drivers

The applications of the AmI technologies mentioned in the scenario have been driven by a set of two or more interdependent factors. Analytically, the following drivers can be distinguished:

- *Political*: The introduction of some of the most important AmI applications in the scenario has largely been driven by political objectives such as reducing the risk of terrorism (security), improving the efficiency of the health care system (emergency), and the improvement of the traffic situation in urban areas (public infrastructure).
- *Commercial*: Numerous AmI services such as the "friend-locator", multimedia applications on the tour bus, individually tailored traffic information and automated communication links are primarily driven by profit motives and the (successful) development of business models.
- *Liability reduction*: Both the boarding procedures at the bus terminal, which proved to be quite humiliating for one of the group members, as well as the fact that hospital patients are required to disclose their complete personal health data, are based on the institutions' objective to reduce liability as far as possible.
- *Illegitimate personal advantages*: As AmI technologies regulate access to scarce goods, people may be motivated to seek personal advantages by circumventing standard procedures and/or by using technical solutions to deceive the system (in the scenario: priority rights in traffic management system). Perpetrators might take into account possible hazardous consequences (because they seek to cause those consequences) or they might not (because they are ignorant of the consequences).

### 8.2.5 Issues

In view of the above-mentioned vulnerabilities of ambient intelligence in travel/mobility and health care applications, we can identify certain issues that are critical for AmI applications that rely on large-scale public infrastructure and have largely the character of a public utility:

*Dependence*

Automated alerts are not necessarily beneficial – they may even cause more confusion because alerts reach the addressee immediately, but direct communication with the victim is often no longer possible.[126] The promise of permanent accessibility leaves the user helpless when communication is needed but not possible.

*Privacy*

What is the necessary degree of disclosure of information? In a normal situation, even the disclosure of simple data (e.g., location) may violate privacy, whereas in other cases, the revelation of more information of the same kind may be warranted. Thus, the degree of information disclosure depends on the person, context and situation, which poses a challenge for the design of adequate communication rules.

*Loss of control*

If certain activities rely on the proper operation of technical systems, a feeling of uneasiness and loss of control may occur if it is not transparent to the citizen why a certain decision is made, especially when common sense suggests a different decision.

*Risk and complexity*

If AmI systems that are vital for the public (such as in emergencies) are known to be vulnerable or that don't cover the whole population, a "conventional" backup system, which provides at least a basic level of service, is needed.

*Safeguards*

Responsibility is moved to the weakest link in the chain, normally the citizen. In cases in which users do not adapt fully to the system requirements (e.g., provision of data); a liability may be generally refused – even if it has nothing to do with a certain damage or harm.

*Exclusion*

Services that are regarded as public utilities today may become commercialised. Even if the common welfare is increased, there is the risk of more inequality and even a loss of benefits for certain social groups (AmI divide).

*Identity*

The loss and/or confusion of identity may not only be the result of malicious identity theft, it can also occur by mistake if the identification of a person is merely based on a detachable personal device.

[126] Savidis et al. 2001 assume in their scenarios that the personal communication device is deactivated for public communication in order not to disrupt emergency relief activities.

*Crime and complexity*

Complex and distributed technical systems may offer new opportunities for illegal activities. This not only applies to property offences and terrorism but also to misdemeanours and regulatory offences. Especially in those cases in which sensitive elements of the public infrastructure (e.g., traffic management) increasingly rely on AmI technology, even minor violations of the rules can unintentionally cause severe damage.

### 8.2.6 Legal synopsis

*Conflict of laws*

In an AmI world, people will be able to enjoy every service everywhere. In the scenario, an example is provided of how a group of elderly people is able to enjoy health and mobility services across borders. If an accident happens, however, it appears that important legal issues arise. Not only are many different service providers involved, these different service providers can provide their services from anywhere in the world. In order to be able to determine who will be responsible for the damage, we have to know which law is applicable and which courts will be competent. At the European level, solutions are provided for contractual and extra-contractual (tort) liability, but they are not adapted to an AmI world.

When considering the criminal issues, the jurisdiction is still determined by national law. Although some instruments try to make uniform computer-related criminal offences, they remain limited in scope and only applicable to a few countries. The legal instruments related to criminal law also deal with people who indirectly make the offences possible.

*Interoperability*

In order to ensure the interoperability between the different services and systems, international standards need to be created. Both at the European and international levels, important efforts are required. The European Union provides for mechanisms to stimulate the Member States to co-operate with each other and with the Union. As shown by the scenario, this cannot solve everything. In order to be able to comply with international standards, everybody needs to have and be able to afford the necessary up-to-date technology. It is unacceptable that some people could not enjoy health and general alarm services because they can not afford the appropriate technology. Not being able to use the necessary health services might have fatal consequences. Stringent regulation should be imposed on health service providers and health insurance companies to guarantee everyone's access to the necessary technology.

*Data protection*

In an AmI world, huge amounts of information will be collected in order to provide personalised services. Several principles of data protection are very important. The first is the proportionality principle, which states that “the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.” However, this principle is obviously at risk in a high-speed society with constant intelligent processing of large amounts of personal data. In other words, disproportionate data processing often takes place. Data processors must also ensure that the personal data are

accurate, up-to-date and correctly processed. Effective methods to object to errors in the data processing should be guaranteed.

Data processing can be made legitimate when the data subject gives her informed consent. The hospital example, however, shows that this consent is often not freely given because the data subject is in a subordinate situation. In more general terms, data subjects are subject to the power of the data controller, who possesses a good or a service to which they want access. When people refuse to consent to the collection of their data, this should not have a negative impact on their situation. The data subject can have legitimate reasons to refuse it (such as fear of spamming) and the hospital cannot limit its own liability because of this legitimate refusal.

## 8.3 CONCLUSIONS

The scenario makes clear that even in fields with a quasi-public character; it is not self-evident that all citizens will benefit from the deployment of ambient intelligence.[127] In fact, the complexity of large-scale technological systems for traffic management and public health shows that careful steps have to be taken in order to balance public and private interests – ranging from government, commercial network and service providers to the individual citizen and civil society as a whole.

It is a great challenge to avoid unjustified and excessive drawbacks or benefits for any of the affected parties. The challenge requires a blend of legal, organisational and technical measures. On the technological level, interoperating systems with a high degree of dependability (supplemented in part by independent backup systems) are needed when the individual or society as a whole depends on an operating system. On the organisational level, measures are needed to make (public) services transparent and trustworthy. Finally, the legal framework and the regulation of important public services have to be adjusted to new circumstances. This also means that existing networks and constellations of societal actors need to respond accordingly.

[127] See, for example, IST Advisory Group, *Ambient Intelligence: From Vision to Reality*, Luxembourg: Office for Official Publications of the European Communities, 2003. http://www.cordis.lu/ist/istag-reports.html. See also Emiliani, P.L., and C. Stephanidis, "Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities", *IBM Systems Journal* 44, No. 3, 2005, pp. 605-619.

# 9 THREATS AND VULNERABILITIES

In this chapter, we present a review of threats and vulnerabilities that could afflict society and individuals in the AmI world in the context of the key policy issues of privacy, identity, trust, security and digital divide.

We define a **vulnerability** as a flaw or weakness in a system's design, its implementation, operation or management that could be exploited to violate the system and, consequently, cause a threat. Vulnerabilities may have different dimensions: technical, functional or behavioural. A **threat** is the potential for one or more unwanted consequences caused by a circumstance, capability, action or event that could be harmful to a system or person. Threats can be caused naturally, accidentally or intentionally. In essence, a threat is a ubiquitous phenomenon.[128]

As will be apparent in the pages that follow, we foresee that many of the threats and vulnerabilities that afflict us now will also afflict the AmI world. Or, to put it differently, based on our research so far, we have discovered few threats and vulnerabilities that could be described as unique or new. To be clear about this, we mean *classes* or *types* of threats and vulnerabilities. In saying so, we do not in any way mean to assuage the AmI enthusiasts. It's been said that, if left unchecked, AmI could obliterate privacy[129], but this is not a *new* threat. Our privacy has been eroding for a long time. By the time, a full-blown, all-singing, all-dancing AmI world is truly upon us, there may not be much left to obliterate. Similarly, it's been argued (and is argued in our reports too) that AmI threatens the individual with a loss of control – if an intelligent environment surrounds us, we may cede much of our control over it to the intelligence embedded everywhere. But this loss of control phenomenon is not new either. We have already ceded a lot of control over our lives to the government and the corporate warlords who pillage consumer society today. What is different about AmI is the scale of the data that will be available. When everything is embedded with intelligence, when AmI is pervasive, invisible, ubiquitous, when everything is connected[130] and linked, the threats and vulnerabilities that we know today will become even greater risks than they are now.

## 9.1 PRIVACY

The notion of privacy is unstable, complex, difficult to fix. People's perception of privacy is context-dependent, in time and space. Our expectations of privacy may be different according to our age, gender, culture, location, family history, income, educational level and many other factors.[131] And governments' perception of what our privacy should be may be different from ours. It is no surprise that scholars understand privacy in different

[128] Xenakis, C., and S. Kontopoulou, "Risk Assessment, Security & Trust: Cross Layer Issues", Special Interest Group 2, 2006, p. 14.
[129] Brey, Philip, "Freedom and privacy in Ambient Intelligence", *Ethics and Information Technology*, Vol. 7, No. 3, 2005, p. 165.
[130] Cf O'Harrow, Robert, *No Place to Hide*, Simon & Schuster, New York, 2005, p. 107: "We have created a unique identifier on everybody in the United States," said [Ole] Poulsen, the company's [Seisint Inc.] chief technology officer. "Data that belongs together is *already* linked together." *[Italics added.]*
[131] See Gutwirth, Serge, *Privacy and the Information Age*, pp. 5-31 ("Privacy's complexities").

ways; some argue that autonomy and liberty are the values behind privacy, while others contend it is intimacy, confidentiality or the control over personal information.[132]

The threats to our privacy, however we define it, can come from many different sources – from prurient neighbours, industry, government, Internet service providers, private detectives and hackers as well as our supposed friends or family.

In a world of ambient intelligence, the threats to our privacy multiply. In an AmI world, we can expect to be under surveillance ("transparent") wherever we go because the permanent and real-time registration and processing of our presence and behaviour is the precondition – the "code" – of ambient intelligence. The further development of an adaptive and intelligent environment of pervasive and ubiquitous computing is, in fact, dependent on intensive automatic processing of behavioural and thus personal data and, hence, of intensive registration and monitoring. Already, video cameras are mounted almost everywhere in London. It's been said that people in that city are recorded on camera more than 300 times a day.[133] With machine learning and intelligent software, our behaviour and preferences can be predicted. Like our credit cards, RFIDs can be used to monitor what we buy. Networking sensors can monitor what we are doing.[134] Mobile phone companies can monitor where we are. Amazon, Google, the credit card companies know lots about us. And who can slow down the voracious appetite of government to know more about us than all of them put together?

ISTAG posed a challenge for researchers, which can be paraphrased as follows: How can we ensure that personal data can be shared to the extent the individual wishes and no more? It's not an easy question to answer. Some safeguards can be adopted, but the snag is that profiling and personalisation, as noted above, is inherent in AmI and operators and service providers invariably and inevitably will want to "personalise" their offerings as much as possible and as they do, the risks to personal information will grow. While there may be, to some extent, safeguards to help contain the risk (but the risk will never be eliminated), there are many unresolved issues. For example, in AmI networks, there are likely to be many operators and service providers, some of whom may be visible, some of whom will not be. Will consumers need to or even be able to negotiate their level of protection with each one? Will some services be on a "take-it-or- leave-it" basis? If you want a particular service, will you have no choice except to forego some of your privacy? Are the privacy policies of operators and service providers satisfactory from the consumer's point of view? Can they be trusted? Are the data protection safeguards put in place by the operator or service provider adequate? If new AmI networks have a profile-learning capability, will the "negotiated" privacy protection rules be relevant after a year or two of service? Will the network players be able to offer different levels of protection to different customers? Are new safeguards going to be effective or will they simply be closing the barn door after the horse has already bolted – i.e., is there already so much

---

[132] See the discussions in Claes, Erik, Anthony Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Intersentia, Antwerp/Oxford, 2006.

[133] See Jordan, Mary, "Electronic Eye Grows Wider in Britain", *The Washington Post*, 7 January 2006: "People in Britain are already monitored by more than 4 million closed-circuit, or CCTV, cameras, making it the most-watched nation in the world, according to Liberty. The group said that a typical London resident is monitored 300 times a day."

[134] "Cybernetic systems that contextualise, learn and act autonomously present fascinating challenges," says the *ARTEMIS Strategic Research Agenda*, First Edition, March 2006, p. 8.
http://www.artemis-office.org/DotNetNuke/PressCorner/tabid/89/Default.aspx

personal information about us "out there" that data miners can already find most of what they want?

### 9.1.1 Threats

Threats to our privacy come from lots of sources. Here are some of the principal ones that affect us today and we can assume will still be threats in an AmI world. Many of these threats are also threats for identity and security.

#### *Hackers*

Today's networks, interconnected by the Internet, frequently are attacked by hackers who engage in spoofing, phishing, denial of service attacks via worms, Trojans, viruses and other assorted malware. Even companies that provide security services have been exposed to breaches in their own security.[135]

AmI networks will supply data aggregators with massive amounts of data from new sources such as so-called "smart dust" networks, RFIDs and the intelligent software driving the new 4G networks. As the scale of data aggregated expands exponentially, there will probably be an increasing concentration and rationalisation in the industry as well as in the databases of governments intent on national ID schemes featuring biometrics including DNA data. The giants among the AmI data aggregators will undoubtedly present irresistible targets to hackers just as Microsoft does today.

#### *Function creep*

Function creep occurs whenever data are used for a purpose other than that for which they were originally collected. The economic logic behind such activity is obvious. It provides efficiencies and savings in cost and effort. Being able to reuse personal data presents a great temptation to industry and government. As AmI penetrates our environment and daily regimes, the amassed data will present new opportunities that were not even dreamed of. In some instances, the individual will benefit from greater personalisation of services and lower costs. In other instances, she will find some of the new services encroaching further upon her sense of privacy and the protection of her personal data.

AmI will give great impetus to function creep. It's been said that whatever can be linked together will be linked together, and therein lies the opportunities and temptations for function creep.

[135] Guidance Software -- the leading provider of software used to diagnose hacker break-ins -- has itself been hacked, resulting in the exposure of financial and personal data connected to thousands of law enforcement officials and network-security professionals. In December 2005, Guidance alerted its customers that hackers had broken into a company database and made off with approximately 3,800 customer credit card numbers. In March, data aggregator LexisNexis acknowledged that hackers had illegally accessed information on more than 310,000 consumers, an attack that was later determined to have been launched after hackers broke into computers used by at least two separate police departments. Krebs, Brian, "Hackers Break Into Computer-Security Firm's Customer Database", *The Washington Post*, 19 Dec 2005.

### *Surveillance*

Surveillance is increasing in the streets, buses, Underground, shops, workplace and on the motorways. Hence, it is now almost impossible to go outside your home without coming under surveillance.

Location-based services form a kind of surveillance. Mobile phone operators and industry have developed emergency service telephone numbers, which can be activated automatically and which will inform the network of the physical location of the user. New electronic services, such as those offered by uLocate and Wherify Wireless, provide the physical location of mobile phone users.[136]

One can imagine a day when almost everyone will have implantable devices, not only for monitoring their physiological condition, but also for tracking their whereabouts. At the same time, there may be considerable social pressure, perhaps even legal requirements, for individuals to bear such implants as a security measure. One could further foresee such implants interacting with the "intelligence"-embedded, networked environment too.

AmI devices such as implants or technologies that monitor our physiological condition and behaviour could well make our society more secure, particularly if they enable law enforcement authorities and intelligence agencies to take preventive measures. Preventive actions by the police are featured in the Spielberg film *Minority Report*, but is this the kind of society we want? More control in order to prevent criminal acts, detect offenders and punish them may be counterproductive for society as a whole. In 1968, the philosopher Heinrich Popitz wrote a classic text on the "preventive effects of nescience" in which he argues that too much (precautionary) knowledge destabilises society, leads to a climate of distrust and finally to more instead of less crime. A world where every breach of the rule is detected and punished can only be hell.

### *Profiling*

Companies such as Amazon keep track not only of their customers purchases, but also their browsing, and with the accumulation of such data, they can build up increasingly accurate profiles of their customers in order to offer them other products in which they might be interested. Search engines keep a log file that associates every search made on its site with the IP address of the searcher. And Yahoo uses similar information to sell advertising; car companies, for example, place display advertising shown only to people who have entered auto-related terms in Yahoo's search engine.[137] Companies such as Doubleclick are specialised in building and analysing profiles by placing cookies on our personal computers and keeping track of our surfing behaviour across numerous affiliated websites.

Customer-supplied data, the data obtained from monitoring purchasing habits and surfing behaviour, and the data obtained from third parties, can also be used to implement dynamic pricing and behavioural targeting. Dynamic pricing, a modern incarnation of price

[136] See Harmon, Amy, "Lost? Hiding? Your Cellphone Is Keeping Tabs", *The New York Times*, 21 Dec 2003: "We are moving into a world where your location is going to be known at all times by some electronic device," said Larry Smarr, director of the California Institute for Telecommunications and Information Technology.
[137] Hansell, Saul, "Increasingly, Internet's Data Trail Leads to Court", *The New York Times*, 4 Feb 2006.

discrimination, means that different prices are offered to customers based on their characteristics.[138]

The unbounded use of personal data for profiling purposes easily leads to self-fulfilling prophecies. People will only see the choices presented to them on the basis of their profile, which leads to choice within these boundaries, and this in turn may lead to refinements in their profile.[139]

Use of the same identifier across multiple transactions can yield comprehensive profile information to the service provider on the usage, interests or behaviour of the user, by linking all available information, possibly from both the online and offline worlds. [140]

Security expert Bruce Schneier has pointed out flaws with profiling schemes. "Profiling has two very dangerous failure modes. The first one is … the intent of profiling … to divide people into two categories: people who may be evildoers … and people who are less likely to be evildoers... But any such system will create a third, and very dangerous, category: evildoers who don't fit the profile… There's another, even more dangerous, failure mode for these systems: honest people who fit the evildoer profile. Because actual evildoers are so rare, almost everyone who fits the profile will turn out to be a false alarm. This not only wastes investigative resources that might be better spent elsewhere, but it causes grave harm to those innocents who fit the profile… profiling harms society because it causes us all to live in fear...not from the evildoers, but from the police… Identification and profiling don't provide very good security, and they do so at an enormous cost."[141]

The PRIME project has echoed this sentiment: Unbridled data collection and profiling by the State in the name of protecting (national) security may lead to unjust and ultimately unwarranted blacklists, however noble the intentions may be. This happens not only in totalitarian regimes, but also in free societies.[142]

---

[138] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 10.
http://www.prime-project.eu.org/public/prime_products/deliverables/
For a practical example of how mobile phone companies engage in differential pricing, see Richtel, Matt, "Suddenly, an Industry Is All Ears", *The New York Times*, 4 March 2006: "When a [Cingular call centre] representative answers the phone, an information page pops up that includes the caller's name and number, whether he or she has called in the last five days, and why that call was made. In the top right of the screen are two icons — one indicating whether the caller is a threat to quit service (largely a measure of whether the customer is still under contract), and the other showing how much money the caller spends each month (a measure of the customer's value). Before long, the screen indicates if the customer is profitable. If a customer is not very profitable, the company may be less likely to make concessions."

[139] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 11.
http://www.prime-project.eu.org/public/prime_products/deliverables/

[140] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 14.
http://www.prime-project.eu.org/public/prime_products/deliverables/

[141] Schneier, Bruce, "Identification and Security", Crypto-Gram Newsletter, 15 Feb 2004.
http://www.schneier.com/crypto-gram-back.html. George Clooney provided us with a recent reminder of this in his recent film, *Good Night and Good Luck*, about Joe McCarthy, who professed that he was making America more secure by exposing Communists and their sympathisers, when in reality he was instilling fear and paranoia across society.

[142] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 11.
http://www.prime-project.eu.org/public/prime_products/deliverables/

### 9.1.2 Vulnerabilities

In addition to the threats highlighted above, privacy today is subject to various vulnerabilities, among which are the following.

#### *Lack of public awareness or concern about privacy rights*

Many people are unaware of their rights and feel unable to know what actually happens to their data. This is not surprising, given the opacity of the processes. This is a serious vulnerability since it is one that cannot be fixed or addressed until someone becomes aware of it (and exposes it).

Lack of public awareness is one thing, but lack of concern about one's rights or a willingness to trade off some of one's civil liberties for greater security is quite another. Recent public opinion polls published in the US suggest that a majority of the public is not really that concerned about encroachments on their privacy and civil liberties, that they are of view that giving up some privacy or forsaking some of their civil liberties is the price of countering security threats, especially from terrorists.[143]

#### *Lack of enforcement and oversight of privacy rights*

Most people are not even aware that data protection infringements are taking place. If they know or presume that infringement is taking place, they often just don't react (e.g., spam). And even if they do react and want to enforce their rights, most EU legal systems require that their damage must be proven.

Some of our personal data are held by the governments and organisations in our own countries, and some are held in other countries. Some countries may have legislation or regulation that affords relatively good protection of our privacy, while others may have regimes that offer no protection whatsoever.

No matter what the best of the legal regimes say, the complexity of the regulation, incomplete enforcement, and sometimes even conscious decisions by businesses and governments not to comply with the rules render legislation ineffective.[144]

#### *Erosion of rights and values*

The erosion of the right to privacy in the past century has been subtle, incremental, gradual and as relentless as technological advance. In today's surveillance society, where our personal data are not secure and are mined, monitored and captured, people have surrendered the right to be let alone in the interests of greater security (safety of society). For the most part, people have accepted the arguments of law enforcement and intelligence agencies that privacy has to be circumscribed so that they have the tools they need to

[143] Drees, Caroline, "Civil liberties debate leaves much of America cold", Reuters, published in *The Washington Post*, 18 May 2006.
[144] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 12.
http://www.prime-project.eu.org/public/prime_products/deliverables/

apprehend criminals and terrorists and to combat the malicious code that floats around the Internet.

Perhaps most people view privacy as a right that can be sacrificed, at least to some extent, if it leads to greater security. But there are questions whether it *has* led to greater security, questions that are unlikely to be adequately answered before the widespread deployment of AmI networks in the near future.

Some have argued that privacy is fundamental to democracy, whether people recognise it or not. In addition to privacy, values such as autonomy (sovereignty), human dignity, physical and mental integrity and individuality are easily undermined by advanced methods of personal data collection, profiling and monitoring. Other fundamental rights – part of the European Charter of Fundamental rights – can be under pressure in an AmI world without privacy or with just a minimal level of privacy, such as the freedom of thought (brain research shows that neural signals can be transformed into computer data and transmitted over networks), freedom of expression and information (the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers), freedom of assembly and association (location data can reveal assemblies, communication data can reveal associations), the right to education (computer education could become more valuable than alphabetic education), non-discrimination (as a consequence of profiling), integration of persons with disabilities (who have less privacy as a (avoidable) consequence of the system design), and so on.

After some years of experience of living in an AmI world, most people will probably care less than they do even today. But how much or how little they care will probably also be a direct function of how their privacy, their personal data, their communications are abused and/or to what extent they have ulterior motives for minimising their exposure to the authorities (i.e., they really may be criminals or terrorists). Press reports of abuse, of liberties taken with existing laws and constitutional rights must help to stimulate some unease in our society generally, if not outrage by civil liberties groups.

### *Uncertainties about what to protect and about the costs of protection*

Just as privacy is an unstable notion, so it is almost impossible to know what to protect in all contexts, especially in view of the capabilities of data mining and powerful software that can detect linkages that might not otherwise be apparent.

With the emergence and deployment of AmI networks, the amount of data that can be captured from all sources will expand exponentially by many orders of magnitude. Hence, the cost of providing 100 per cent privacy protection may be prohibitive and unrealistic, even if there were some consensus about exactly what it is we wish to see protected.

### *Uncertainties about the economic costs of privacy erosion*

There have been few studies aimed at analysing the value of privacy, either from a corporate point of view or that of the individual.[145] The cost of losing privacy is twofold:

[145] But there have been some. For a list of articles on the economics of privacy, see http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm

On the one hand, one is confronted by the cost of becoming transparent; on the other, one is exposed to the cost of losing control. There is also the cost of new AmI-related crimes such as identity theft. The economic costs, therefore, are not only the design of the system, but also the consequence of the design in the long term.

Certainly, protecting personal data, through security measures, notably in compliance with the EU's data protection directive (95/46/EC), carries a cost. The directive requires data controllers and processors to protect personal data in proportion to "the risks represented by the processing and the nature of the data to be protected" (Article 17.1). Such costs might include the cost of encryption and establishing a range of protection measures, not least of which is training staff. The cost of implementing the information security measures detailed in ISO 17799 could be quite substantial. From a shareholder's point of view, these costs of protecting can be identified, but the value of doing so might be more uncertain. Where's the payback, they might well ask.

There might be some payback in the context of the company's image, i.e., it could say that it complies with ISO 17799 and, accordingly, it might hope or have some expectation that doing so will engender more trust and loyalty on the part of its customers in the company's brand. Even so, doubts must remain as to whether that automatically translates into greater market share or additional profitability. If the company does gain greater market share or additional profitability, the cause might not be the fact that it has taken adequate measures to protect the personal data it holds, but some other factor. As a minimum, the company would need to do some careful market studies to determine what factors led to improvements in its market position.

Some indication of the economic value of privacy can be adduced from the costs borne by companies where there have been breaches of their databases resulting in the theft of personal data. In such cases, companies have had to bear the cost of informing users or subscribers of the breach, of compensating those whose personal data have been compromised, of establishing improved countermeasures, subjecting themselves to independent privacy audits and so on. Recently, ChoicePoint was subjected to a $10 million federal fine over security breaches that exposed more than 160,000 people to possible identity theft. "The message to ChoicePoint and others should be clear: consumers' private data must be protected from thieves," FTC Chairman Deborah Platt Majoras said.[146] Such direct costs are only part of the overall cost equation, however. There are additional costs arising from, for example, damage to the company's image, reputation and name.

If companies have difficulty in assessing the value of their privacy protection measures, the individual is almost surely faced with even greater difficulties. If the individual is being spammed a lot, getting a lot of unwanted e-mail, how easy or difficult will it be to translate the nuisance it causes into cold hard cash? Is it simply the cost of the individual's time in deleting unwanted e-mail? Can a value be ascribed to the anguish the individual might feel in knowing that his contact details are on some spammer's e-mail list?

Those who have been victims of identity theft might have some pretty good ideas of the costs to them, in terms of lost time and perhaps direct financial loss, in trying to recover

[146] Mohammed, Arshad, "Record Fine for Data Breach", *The Washington Post*, 27 January 2006.

from the theft, but still there must be an open question about the stress and anguish caused by the theft and what is the monetary value of such stress and anguish.

Certainly there are social costs too arising from identity theft, but there appears to be no study analysing the costs, even though the number of victims seem to be rather large. The US Federal Trade Commission has estimated the number of victims at around 10 per cent of the population, and the number of victims in the UK, if not the EU as a whole, also has been estimated as increasing, if not yet to such levels.

While the costs of identity theft can be estimated, what is one to say about the costs of, for example, increased surveillance? How does the individual value the supposed increase in security versus the encroachment upon his privacy?

For the individual the value of his personal data must be even more difficult to pin a figure to. For starters, the individual is highly unlikely to be aware of all those organisations that hold some of his data. And even if he were, he would most likely not be able to judge the cost to him of some threat to his privacy arising from the data mining operations and the linkages aimed at either providing him with more personalised services or establishing his culpability in the context of some supposed terrorist threat.

And what of the future? How easy will it be to place a value on what remains of our sense of privacy in 10 years, assuming encroachments continue, compared to the value that might be ascribed today? Is there a formula that can be devised to work out the net present value of privacy today compared with that in the AmI world a decade hence?

### *Lax security*

One of the most serious vulnerabilities facing those who care about their privacy is the lax security put in place to protect personal data and the privacy of communications. A quarter of UK businesses are not protected against the threat caused by spyware, while spyware caused one in seven of the security incidents reported, according to a recent report by the Department of Trade and Industry.[147]

This vulnerability has at least two aspects – one is the increasing sophistication of efforts by hackers, industry and government to acquire or mine personal data unlawfully or to intercept communications. The other is the inadequate measures taken by those who are expected to protect personal data and the privacy of communications.

The prevalence of identity theft in part reflects the failure of many information brokers, retailers and credit issuers to adequately protect records or to do enough to stop criminals who seek them by verifying their identities.

If some good can be seen coming from the many instances of abuse of personal data held by the private sector and government, it is that security issues have become of greater concern to those who are designing and building the AmI networks of the future. On the

[147] Espiner, Tom, "Viruses cause most security breaches", ZDNet UK, 28 Feb 2006. http://news.zdnet.co.uk/0,39020330,39254929,00.htm. Chris Potter, co-author of the report and partner at PricewaterhouseCoopers, said spyware was the hardest threat to detect. He is quoted as saying "Old style attacks just caused indiscriminate damage, like a plane dropping bombs. Now it tends to be a mass of guerrillas attacking organisations to take confidential information, which is much more subtle and insidious."

other hand, offsetting that design awareness is an assumption that future networks are likely to be much more complex than those in place today. And with each additional complexity, there is the potential for exploiting those complexities with malicious intent.

### *Government and industry are less than forthright*

So many people and organisations hold personal data about us, it is virtually impossible to know who they are, let alone to keep track of what they are doing with our data, whether the data they hold are accurate, and how such data may change, be added to, deleted or amended – even though, according to EU data protection legislation, data processors are supposed to notify national authorities of the categories of data processed, the purpose of processing, the retention period and the security and confidentiality measures taken and even though data controllers are expected to notify individuals concerned so that they can access, amend or delete the data. Although these obligations exist, their efficacy has been undermined by the bad faith of some private sector data controllers and because enforcement has not been rigorous.

We should not be surprised by comments made by executives of two major data brokers who acknowledged to a US Senate panel that their companies did not tell consumers about security breaches that exposed more than 400,000 people to possible identity theft.[148] Similarly, governments, notably the Bush administration, have been reticent about domestic surveillance even after *The New York Times* in December 2005 exposed the fact that the US National Security Agency had been spying, without warrants, on thousands of Americans.

## 9.2 IDENTITY

Identity, which potentially includes attributes as well as personal information, is distinctive to a given individual. For example, when a driver's licence is initially issued, an effort is made to bind the driver's licence number to an identity that is distinct enough to be linked, in theory, to the individual who requested the licence. Part of the identity comprises attributes such as eye and hair colour, height, weight, a photographic image of the individual, and so on.[149]

An **identifier** points to an individual. An identifier could be a name, a serial number, or some other pointer to the entity being identified. Examples of personal identifiers include personal names, social security numbers, credit card numbers and employee identification numbers.

Identities have **attributes**. Examples of attributes include height, eye colour, employer, and organisational role.

---

[148] Krim, Jonathan, "Consumers Not Told Of Security Breaches, Data Brokers Admit", *The Washington Post*, 14 April 2005. See also Stout, David, "Data Theft at Nuclear Agency Went Unreported for 9 Months", *The New York Times*, 10 June 2006.

[149] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?: Authentication Through the Lens of Privacy*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academies Press, Washington, DC, 2003, p. 131.

**Identification** is the process of using claimed or observed attributes of an individual to infer who the individual is. Identification can be regarded as a "one-to-many" check against multiple sets of data. **Verification** is the comparison of sets of data to establish the validity of a claimed identity. It is based on a "one-to-one" check.

**Authentication** is the process of establishing confidence in the truth of some claim. Authentication does not necessarily *prove* that a particular individual is who he or she claims to be; instead, authentication is about obtaining a level of confidence in a claim.

**Authorisation** is the process of deciding what an individual ought to be allowed to do.

Identity is associated with an individual as a convenient way to characterise that individual to others. The set of information and the identifier (name, label or sign) by which a person is known are also sometimes referred to as that person's "identity". The choice of information may be arbitrary, linked to the purpose of the identity verification (authentication) in any given context, or linked intrinsically to the person, as in the case of biometrics. For example, the information corresponding to an identity may contain facts (such as eye colour, age, address), capabilities (for example, licensed to drive a car), medical history, financial activity and so forth. Generally, not all such information will be contained in the same identity, allowing a multiplicity of identities, each of which will contain information relevant to the purpose at hand.[150]

Computers have enabled us to digitise all sorts of information including that relating to our identity. Hence, a **digital identity** (or electronic identity, **eID**) is the electronic representation of an individual (or organisation). Digital identity mechanisms are not restricted to smart cards. An eID can potentially operate across different platforms, including, for example, mobile phone SIM cards. Whatever media are used, eID schemes need to be able to authenticate users and to support electronic transactions.

As we can be identified in many different ways, so the concept of **multiple identities** has arisen. We may have multiple identities, which serve different purposes in different contexts. Individuals usually have multiple identities – to family, to an employer or school, to neighbours, to friends, to business associates and so on. Thus, different sets of information are associated with an individual in different contexts. Multiple identities might be better termed as a collection of **partial identities**.

Multiple identities (that is, multiple sets of information corresponding to a single individual) may allow individuals to control who has access to what kinds of information about them. The use of multiple identities can be a legitimate strategy for controlling personal privacy in an information society. In addition to providing a measure of privacy protection, the use of multiple identities, even with respect to a single organisation, serves legitimate and desirable functions in societal institutions as well. [151]

---

[150] Kent, Stephen T., and Lynette I. Millett (eds.), *IDs--Not That Easy. Questions About Nationwide Identity Systems*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academy Press, Washington, DC, 2002, pp. 18-20.

[151] Kent, Stephen T., and Lynette I. Millett (eds.), *IDs--Not That Easy. Questions About Nationwide Identity Systems*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academy Press, Washington, DC, 2002.

To function in the cyber world, people need an identity or multiple identities. In some instances, we can hide behind our cyber identity, that is, to minimise the disclosure of personal information. **Pseudonyms** can be used to mask identity or reveal parts of it for gaining specific benefits such as participation in a loyalty programme, establishing reputation, or proving a legally valid identity in case of dealings with law enforcement. In other instances, this may not be so possible. For example, some service providers, like the government, may require personally identifiable information, so that if we want the service, we must provide the personal data demanded by the service provider.

In some instances, an individual will need to authenticate who he is or will need to authenticate one of his multiple identities. Hence, the individual will need to have some means to choose the appropriate identity to use. In many cases, he will want to avoid linkages. Hence, he will need to be able to access some **identity management system** that will help him to choose the appropriate identity to use in the particular circumstances.

In AmI, identifying a subject is not the only way to act. Persons can be identified indirectly by their accessories, for example, when objects receive unique identifiers. In addition to the identification of objects, biometrics is another important feature of AmI because it uses our body as an identification tool. People can be identified by their veins, fingerprints, iris scans, heart beat, typing behaviour, voice, gait and so on). In theory, this should enhance the comfort of users who don't need to actively identify themselves, thereby reducing ballast (identity papers) and time otherwise consumed by the identification or authentication process.

In an AmI world, we will need to identify ourselves or to use a partial identity in order to use an AmI service, most probably many times a day. In some instances, the identification or authentication process will be as a result of a conscious, deliberate decision on our part, in which case we may use our eID. In other instances, the identification process may happen automatically, without any intervention on our part.

With intelligence embedded everywhere in an AmI world, our identity may mutate from a collection of our identifiers and attributes or from a partial identity which we create to something that is created by our presence in and movement through that world.[152] Our identity could become an accumulation of not just our attributes and identifiers, as it is today, but an accumulation of where we have been, the services we have used, the things we have done, an accretion of our preferences and behavioural characteristics. Future technologies may pinpoint our identity, without our intervention, through some combination of embedded biometrics that identify us by the way we walk and/or our facial characteristics and/or our manner of speaking and/or how we respond to certain stimuli.

[152] Human beings leave a vast amount of processable and thus correlatable electronic traces, generated spontaneously by our presence and movement through the world. New technology enables collection, processing and correlation of this vast amount of data. These evolutions represent more than mere quantitative changes: they induce a significant qualitative shift that can be described by the notions of the 'correlatable human' and/or 'traceable or detectable human'. See Gutwirth S. and P. de Hert, "*Privacy and Data Protection in a Democratic Constitutional State*" in M. Hildebrandt and S. Gutwirth (eds.), *Profiling: Implications for Democracy and Rule of Law*, FIDIS deliverable 7.4, Brussels, 2005, p..26. www.fidis.net. The development of these concepts is the result of networked and interdisciplinary research carried out under the inter-university research project "The loyalties of knowledge", financed by the Belgian Federal Science Policy Office (see www.imbroglio.be). See also Hildebrandt M., *"Profiling and the Identity of European Citizens"* in M. Hildebrandt and S. Gutwirth (eds.), *Profiling: Implications for Democracy and Rule of Law*, FIDIS deliverable 7.4, Brussels, 2005, p. 42. www.fidis.net

Thus, our identities may be determined by our mere presence in the AmI world, whether we agree to being identified or not. Needless to say, this kind of identification process could give rise to a host of security, privacy and trust issues.

Third-party profiling could also compromise our sense of identity in an AmI world too. If our ambient intelligence environment assumes that, based on past activity and preferences, we can be expect to behave in a certain way in the future, we may be presented a course of action which would not have been our first choice. Worse, we may feel obliged to accept the AmI-presented course because it seems what is expected of us.[153] In this way, our sense of identity begins to erode. Such a situation could also be regarded as inimical not only to our personal freedom, but also to democracy itself (this is an instance of the chilling effect which is generally associated with one's recognition that one is under constant surveillance).

ISTAG posed the challenge: How should we manage the relationship between identification and anonymity, so that authentication can be achieved without compromising privacy? It's another tough question, but one that has focused the minds of researchers in several AmI-related projects. Virtually all of these projects agree that identity management and authentication should be easy for users and service providers to understand and use.

Establishing one's identity and avoiding identify theft are important in many sectors. It particularly preoccupies the EC and Member States in their drive to put government online. Proof of citizen identity is a requisite for many e-government services, but so far no standard authentication system is accepted and widely used by citizens. The GUIDE project (Jan 2004-June 2005)[154], which sought to speed up the adoption of e-government across Europe, rightly took the view that services must be citizen-centric, user-driven and technology-enabled, but also recognised the specific needs of Europe based upon the social, ethical and legislative differences regarding privacy and data protection.

Making identity management easy for users and service providers to understand and to use is also a goal of the PRIME project, which aims to develop models demonstrating innovative solutions for managing identities in real life situations, such as travel, location-based services, e-learning and e-health, and thereby bring privacy-enhancing technologies closer to the market.

The identity issue is also a focus of the FIDIS project (Apr 2004-Mar 2009)[155], a network of excellence focusing on seven interrelated research themes:

- the "identity of identity"
- profiling
- interoperability of IDs and ID management systems
- forensic implications
- de-identification

[153] This AmI phenomenon has been described as cognitive dissonance. See Brey, Philip, "Freedom and privacy in Ambient Intelligence", *Ethics and Information Technology*, Vol. 7, No. 3, 2005, p. 162. "Users may even start experiencing cognitive dissonance, when they believe they want one thing but a smart object tells them they want something else."

[154] GUIDE is the acronym for Government User IDentity for Europe. The project has a budget of €12.47 million and 23 partners. Its website is http://istrg.som.surrey.ac.uk/projects/guide

[155] FIDIS is the acronym for the Future of Identity in the Information Society. The project has a budget of €6.10 million and 24 partners. Its website is at: www.fidis.net

- high tech ID
- mobility and identity.

According to the FIDIS consortium, the European Information Society requires technologies which address trust and security yet also preserve the privacy of individuals. As the Information Society develops, the increasingly digital representation of personal characteristics changes the ways of identifying individuals. Supplementary digital identities, so-called virtual identities, embodying concepts such as pseudonymity and anonymity, are being created for security, profit, convenience or even for fun. These new identities are feeding back into the world of social and business affairs, offering a mix of plural identities and challenging traditional notions of identity. At the same time, European states manage identities in very different ways.

## 9.3 THREATS AND VULNERABILITIES IN IDENTITY

### 9.3.1 Threats to identity

Threats to our identity can come from various sources, among which are the following.

#### *Identity theft*

Identity theft (or identity-related crime) is one of the fastest-growing white-collar crimes. Typically someone steals our financial details, most often our credit card details, to commit fraud. The identity thief can impersonate us financially, to take out loans, raid our bank accounts, purchase luxury items. The credit card companies may minimise our losses when purchases are made against our cards (or some facsimile thereof), but we may be liable for the other items. Identity theft can also ruin our creditworthiness even if we are not culpable. It may take a long time, a lot of aggravation, to restore our creditworthiness and recover our financial identity.[156] As serious as identity theft is for us as individuals, the credit card companies feel no less aggrieved and, given the magnitude of identity theft, they have been devoting lots of resource and effort to deal with it. The recent replacement of our signature by chip and pin cards is just one indication of their efforts to combat this form of fraud.

Identity fraud is costing the credit card sector billions of euros each year, and is a major source of privacy complaints.[157] Both MasterCard and Visa monitor Web sites that broker

[156] A survey conducted by Privacy Rights Clearinghouse and the California Public Interest Research Group found that the average victim of identity theft did not find out that he or she was a victim until 14 months after the identity theft occurred and that it took the victim an average of 175 hours to solve the problems that occurred as a result of the identity theft. Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, p. 99.

[157] The FTC said identity theft again topped the number of consumer complaints it received in 2005, as it has in recent years. See FTC press release "FTC Releases Top 10 Consumer Fraud Complaint Categories", 25 Jan 2006. http://www.ftc.gov/opa/2006/01/topten.htm. See also Krim, Jonathan, "Data on 3,000 Consumers Stolen With Computer", *The Washington Post*, 9 November 2005. "Social Security numbers and other information about more than 3,000 consumers were stolen recently from TransUnion LLC, one of three U.S. companies that maintain credit histories on individuals, in the latest of many security breaches that have focused congressional attention on identity theft and fraud."

stolen credit card numbers and other personal information; they've discovered that an identity is worth about $10 on the Internet. [158]

Despite the prevalence of identity theft, prosecutions are rare, and police investigations – when they do happen – are time-consuming, costly and easily stymied. A 2003 study by Gartner Inc. suggested that an identity thief had about a 1 in 700 chance of getting caught.[159]

It is an open question whether ambient intelligence will increase or decrease opportunities for identity theft and fraud. With orders of magnitude of more personal information generated in an AmI environment, one might not be too hopeful that the problem will go away. On the other hand, if some privacy-enhancing technologies, like those proposed in the PROGRESS Embedded Systems Roadmap or in the PISA and PRIME projects, are developed and become widely available, one might think the consumer will have better defences against at least some forms of identity theft.[160]

But technology can only help to some extent. Gullibility and carelessness, human traits, are less easily fixed.

### *Function creep*

The data protection directive 95/46, which is not applicable in areas of criminal law and state security, defines an identity and any information related to an identified or identifiable *natural* person as personal data. Identification is the processing of personal data and therefore falls under the principles of data protection such as the principle of purpose specification and use limitation (use conforms only to the original purpose).

The growing awareness of identity theft has prompted many businesses to require customers to provide identification information, especially online and over the telephone. Identification information can come from passports or ID cards or drivers' licences as well as biographical data such as date of birth or mother's maiden name or from biometrics like fingerprint or iris scans. In attempts to minimise the risk of identity theft and fraud, businesses may be increasing privacy risks.

Even if the choice is made to implement authentication systems only where people *today* attempt to discern identity, the creation of reliable, inexpensive systems will invite function creep – the use of authentication systems for other than their originally intended purposes – unless action is taken to prevent this from happening. Thus, the privacy consequences of both the intended design and deployment and the unintended, secondary uses of

---

[158] O'Brien, Timothy L., "Identity Theft Is Epidemic. Can It Be Stopped?" *The New York Times*, 24 Oct 2004.
[159] Zeller, Tom Jr, "For Victims, Repairing ID Theft Can Be Grueling", *The New York Times*, 1 Oct 2005.
[160] The term privacy-enhancing technologies (PETs) represents a spectrum of both new and well-known techniques to minimise the exposure of private data, for users of electronic services in the information society. Currently, no widely accepted definition of privacy-enhancing technologies has been established, but one can distinguish technologies for privacy protection (psydeunomizer, anonymizer and encryption tools, filters, track and evidence erasers) and for privacy management (informational and administrational tools). See e.g. Koorn, R., H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen and J. Borking, "Privacy-Enhancing Technologies. White Paper for Decision-Makers", The Hague, Ministry of the Interior and Kingdom Relations, 2004. http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

authentication systems must be taken into consideration by vendors, users, policy makers and the general public.[161]

It is not hard to see signs of function creep when we travel from one country to another. The US, the UK, Japan and other countries are introducing biometric requirements to supplement passport data. The UK has introduced iris scanning, supposedly to speed passengers through immigration controls. The scan is linked to their passport details. Now the government will have one more bit of data about UK and other citizens who chose to participate in the scheme. For its part, Japan, like the US, has decided to fingerprint and photograph visitors. Gathering such biometric data is grist, not just for civil aviation authorities, but also for law enforcement, the intelligence agencies and controlling immigrants. It's the same with loyalty cards that supermarkets foist on their customers. Such cards are purportedly to reward loyal customers when in reality they serve the market research and marketing departments. Such cards strip away the anonymity of cash-paying customers, enabling the supermarket chains to better target and spam customers.

As AmI becomes pervasive, at least in developed countries that can afford such networks, the opportunities for supplementing basic identifier data will surely grow.

### *Exploitation of linkages by industry and government*

Even among those who understand the benefits of partial identities, it will be miraculous if they can avoid usage of at least one attribute across those partial identities. Only one attribute shared by two partial identities is needed to establish a link between them and all the other attributes. It could be a telephone number, an e-mail address, a date of birth, almost anything will do.

An AmI world will be a highly networked world, which will facilitate linkages between different networks. Hence, where today it is possible to have multiple partial identities that correspond to our different roles in society – as neighbour, employee, student, etc – AmI will facilitate linkages between these different partial identities leading to a great increase in their integration. Both government and industry, despite any protests to the contrary, will find it irresistible to facilitate such linkages for their own, sometimes nefarious, purposes. The more linkages that can be established, the more government and industry will know about us, our behaviour patterns, what we are doing, where we are at any given moment, our disposition towards particular products or services or activities some of which may be deemed as socially unacceptable.

From the individual's point of view, however, more linkages will raise more concerns about the security and protection of our personal data. It may also lead to an erosion of trust – how much trust are we likely to place in Big Brother and a host of "little brothers" when we feel they know almost as much about us as we do ourselves.

### *Penetration of identity management systems (hacking, spoofing, DOS, etc)*

Identity management systems are subject to many of the attacks common to other Internet or computer-communications-based systems, such as hacking, spoofing, eavesdropping and denial of service.

[161] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?,* p. 29.

Some authentication systems make it possible to identify an individual without the individual's consent or even knowledge. Such systems deny the individual, and society, the opportunity to object to and to monitor the identification process. These technologies are particularly vulnerable to misuse because their use is hidden.[162]

There's no reason to think these sorts of attacks that plague us today are likely to go away in an AmI world.

### 9.3.2 Vulnerabilities in identity

In addition to the threats mentioned above, identity management systems may exhibit certain vulnerabilities, such as the following.

#### *Authentication may intrude upon privacy*

A US National Research Council report has warned that authentication technologies could intrude upon privacy in different ways. Authentication methods may require contact with or close proximity to the body, potentially raising concerns under the "bodily integrity" branch of privacy law. Authentication may introduce new opportunities to collect and reuse personal information, intruding on "information privacy". Authentication systems may be deployed in a manner that interferes with individuals' "decisional privacy" by creating opportunities for others to monitor and interfere with important expressive or other personal activities. Authentication methods may raise new opportunities to intercept or monitor a specific individual's communications, revealing the person's thoughts and the identities of the individuals with whom he or she communicates.[163]

#### *Complexity of identity management systems*

Governments and industry have been developing a multiplicity of identity management systems for various purposes, with the intent of putting more (or virtually all) of their services online or, in the instance of the rationale for national ID cards, for combating fraud and terrorism. Some systems, for example, the UK's Inland Revenue system that permits individuals to file their tax returns online, are becoming very big indeed with millions of files. Eventually the national ID card scheme will become even bigger. If common standards are agreed for national ID systems across the EU, an EU ID card may not be long in coming. Inevitably, as the systems and their attendant databases become bigger, the complexity of the systems grows.

The multiplicity and complexity of such systems offers a possible foretaste of what identity management could become like in an AmI environment, when there will be many more systems, networks and services on offer. While there are some who believe that a single sign-on approach would reduce (somewhat) the complexity of interacting with a multiplicity of systems, others believe a decentralised approach reduces the risk that might arise from a massive failure or attack on a centralised system.

[162] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, pp. 30-31.
[163] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, p. 63.

The snag with the growing complexity of computer communications systems, including those that will form the backbone of AmI networks, is that vulnerabilities increase with complexity. Experience has taught that systems — and, in particular, complex systems like networked information systems — can be secure, but only up to a point. There will always be residual vulnerabilities, always a degree of insecurity.[164]

### *Failures in identity management systems & authentication systems*

If intelligence is embedded everywhere in an AmI world, there will be lots of people, companies, organisations collecting identity data. So questions will arise about their securing of our data. How well will supermarkets, or the corner grocery store, protect our identity data?

Security expert Bruce Schneier has said that it doesn't matter how well a system works, what matters is how it fails. No matter what their merits may be, if identity management, authentication and authorisation systems generate a large number of false positives, i.e., they authenticate or authorise someone to engage in some transaction when he shouldn't be permitted to do so, they will be regarded as failures.

It may be assumed that biometrics will ultimately reduce the number of false positives in view of the supposedly unique nature of each set of fingerprints, irises and other physiological features, but false positives are still possible. Sometimes these false positives are generated not by the technology but by those who wield the technology, as happened when the FBI became convinced, wrongly, that they had identified an Oregon lawyer, a Muslim convert, as a participant in the terrorist attack on Madrid trains in March 2004, on the basis of a single fingerprint which was a near match to one found in Madrid.

Problems like this *could* be reduced if AmI networks generate so much data about the individual that the individual is virtually unmistakeable. But if we arrive at that situation, it may also mean that there is a significantly greater amount of personal information floating around, so that the capture and analysis of such information reduces the very protection of privacy that identity management systems are supposed to support.

### *People do not take adequate care to protect their cyber identity(-ies)*

Today cyber citizens often use the same password or ID over different websites and systems, which is bit like writing down passwords on bits of yellow paper stuck on the side of computer screens: such actions undermine the point of having passwords. Unconsciously or not, most cyber citizens today do not take adequate care to protect their identity or identities. Some of the privacy-enhancing technology schemes that are being considered for today's cyber world and that of the AmI world may help reduce this problem, but it's unlikely to go away. Human nature, being what it is, means that some people just will not take even the most basic of steps towards protecting themselves. From this optic, identity theft may have a salutary effect of being a good learning experience, but this is a bit like saying that walking with your eyes closed across a busy street can be a good learning experience. In any event, once the theft has occurred, it may be as difficult or impossible to recover from as being run over by the number 9 bus.

---

[164] Committee on Information Systems Trustworthiness, *Trust in Cyberspace*, National Research Council, National Academies Press, Washington, DC, 1999, p. 119.

### *Misplaced trust in security mechanisms*

Any technology, including single sign-on, that requires you to relinquish control of your personal information should be regarded as a risk. Despite that risk, we may believe or we have been convinced that AmI PETs will protect us. In doing so, we may be trusting security mechanisms that don't warrant our trust. In some cases, particularly where we are required by law and/or by law enforcement authorities, we may be forced to rely on (to trust) the adequacy of security mechanisms, of others' privacy policies.

This is the situation in which we find ourselves with regard to national ID card schemes. Despite the criticisms voiced in the UK elsewhere about such schemes, Britons almost certainly, despite rearguard efforts by the House of Lords, will be forced to get a national ID card.

The national ID card has been criticised on many grounds, including cost. But in terms of security, Stella Rimington, a former director of MI5, has cast doubts on their efficacy as a security measure against terrorism. Security expert Bruce Schneier has said, "The potential privacy encroachments of an ID card system are far from minor. And the interruptions and delays caused by incessant ID checks could easily proliferate into a persistent traffic jam in office lobbies and airports and hospital waiting rooms and shopping malls. It won't make us more secure… No matter how unforgeable we make it, it will be forged… And even if we could guarantee that everyone who issued national ID cards couldn't be bribed, initial cardholder identity would be determined by other identity documents... all of which would be easier to forge… But the main problem with any ID system is that it requires the existence of a database… Such a database would be a kludge of existing databases, databases that are incompatible, full of erroneous data, and unreliable. As computer scientists, we do not know how to keep a database of this magnitude secure, whether from outside hackers or the thousands of insiders authorized to access it… A single national ID is an exceedingly valuable document, and accordingly there's greater incentive to forge it."[165]

In an AmI world, we may find an analogous situation, where identity management solutions are promoted by governments who expect us to take on trust that their solutions are inherently safe and secure. Many of us may accept their logic and blindly put their trust in the proposed solution until hard experience teaches us otherwise.

## 9.4 TRUST

In engineering visions of ambient intelligence, technology is invisible in practice, functioning silently in the background – this entails the search for perceptual transparency in interaction – the tool itself should be invisible, non-focal, while the tasks and results are ready-to-hand.[166] This may lead to a conflict between the goals of opacity and

[165] Schneier, Bruce, "National ID Cards", *Crypto-Gram Newsletter*, 15 Apr 2004. http://www.schneier.com/crypto-gram-back.html

[166] Weiser, M., and J. S. Brown, "The Coming Age of Calm Technology", in P. J. Denning and R. M. Metcalfe (eds.), *Beyond Calculation: The Next Fifty Years of Computing*, Copernicus, New York, 1997, pp. 75-85; Aarts, E., R. Harwig and M. Schuurmans, "Ambient Intelligence", in P. Denning, *The Invisible Future: The Seamless Integration of Technology in Everyday Life*, McGraw-Hill, New York, 2002, pp. 235-

transparency/invisibility. As technologies that exist in the background are deliberately designed to be transparent and invisible, they may also bring with them a kind of distrust that, rather than being manifest, is latent and potential. While technological transparency is thought to provide the ideal task-oriented situation, it also effectively black-boxes the overall technological environment, makes it opaque and intangible, complicating trust based on a disclosure of intentions and qualifications in that it hides its presence, and becomes absent – something that is somehow there, but unseen, working tacitly, perhaps unsettlingly, in the background. The intentions and the power relations implemented in the system and the way the system works on more than a mere task level is effectively concealed, and observation, control and empowering of inhabitants are withheld. This leaves no room for a "place" for interaction, no node where action can be taken, and the system, and all that it entails, judged or contemplated. Not only does the background "presence-in-absence" status of such systems raise concerns about privacy and data access ("Who controls the data I give out? Who watches me now?"), but arguably they also complicate the giving out of trust because the object, the other or some index of presence is missing. The direction of trust, then, is free-floating, abstract and distributed, rather than localised, visible and embedded in present situations.

ISTAG posed the challenge: What measures are there, and what standards should there be for dependability, trustworthiness, privacy?

None of the projects reviewed by SWAMI specifically focuses on trust from the point of the individual AmI user, on how user trust can be earned or what measures must be taken in order to gain the confidence of the user and satisfy her concerns about particular technologies. The issue of trust from the user's perspective would seem to merit greater consideration and more detailed study than heretofore has been the case.

One of the most important inhibitors to public acceptance of the Internet for human interactions (commercial or otherwise) has been the lack of trust in the underlying cyber infrastructure and in other people whom we meet through that infrastructure. Incidents of massive identity theft from otherwise internationally trusted financial institutions, the never-ending resourcefulness of malicious hackers, intruders and spammers, have increased the apprehension and uneasiness of the general public vis-à-vis the Internet and the Web – and there is strong evidence that this will apply to an even greater extent to ambient intelligence services in the future.

It is a challenge to change this climate not only at the level of interactions among human agents (commercial or otherwise) through the use of the cyber infrastructure, but also among human and software agents. This is a grand challenge, since the "mechanics of trust" may vary drastically between different cultures. Moreover, there are trade-offs between trust and privacy, trust and security, and trust between commercial competitors that are not easily brought to a balance.

In the following, threats to and vulnerabilities in trust are discussed with regard to four areas: inadequate profiling, loss of control, service refusal and discrimination, and victimisation. These areas are closely interrelated. For instance, poor profiling is a problem because the promised customisation might be deficient and, at the same, because it

---

50; Streitz, N. A., and P. Nixon, "The Disappearing Computer", *Communications of the ACM*, Vol. 48, no. 3, 2005, pp. 32-35.

represents a precondition for certain denials of services. Thus, distinctions between the four areas have been introduced for analytical purposes. Moreover, as the concept of trust is multi-dimensional, largely intangible and encompasses interdependent relationships, problems primarily related to privacy, identity, security and the digital divide are relevant for the issue of trust as well.

### 9.4.1 Inadequate profiling

As the AmI vision is geared towards a user-driven approach, one of the key means of meeting the users' individual needs is personalisation. In order to be able to deliver customised services, user-specific profiles need to be created. Profiling in an AmI environment consists of constantly collecting and processing a broad range of data from numerous sources that are related to a user's identity, his/her activities, characteristics and preferences in specific environments. Based on constructed profiles, AmI systems able to respond to the users' needs – or at least what is assumed to be their needs inferred from the interpretation of the collected information. Problems of inadequate profiling can occur in two main situations: attribution conflicts involving numerous users and misinterpretation of users' needs.

#### *Multiple users*

In the case of incorrect attribution, two or more users are concurrently present in an AmI environment. The users' profiles, actions and preferences may not necessarily be congruent.[167] If profiles are completely or even partially incompatible, conflicts over shared services and resources might occur. If these conflicts are not resolved adequately, user acceptance is at stake. A possible solution is to average out the disputed profile parameters. However, in many areas of daily life – for example, where users have different musical preferences – such simple mathematical remedies are not feasible.

#### *Misinterpretation of needs and inadequate expression of preferences*

The quality of a personal profile depends both on the scope and depth of the input data as well as on the adequacy of the data processing. However, even if service providers decide to invest sufficient resources into the continuous monitoring by numerous sensors and the development of "intelligent" software in order to improve the performance of an AmI system, the profiles developed from the collected data represent – at best – constructed approximations of the actual user preferences. Information collected by AmI sensors is mainly based on observed patterns of behaviour. Thus, just as in the case of empirical social research, profiling can merely capture a simplified extract of a complex reality; moreover, the data tend to be distorted by artefacts. In short, linking observable behaviour to an individual's intentions is highly problematic and prone to misleading interpretations – a challenge, of course, faced by every developer of an "intelligent" system.

The most common approach to ease the problem is to supplement the profiling process by requesting direct input from the user. However, this is not only at odds with one of the envisioned key characteristics of AmI – namely the disappearance of user interfaces – it also entails other considerable trade-offs. The predefined choices can either be very

[167] Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick, "Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence", FIDIS Deliverable D7.3, 2005, p. 12.

limited, hence constraining users' options profoundly. Or, if the opposite strategy is implemented and very detailed choices are offered, the user is burdened with time consuming and perhaps annoying adjustment and programming procedures. Moreover, this method can only be successful to the extent that the user is, firstly, cognisant of her/his preferences and, secondly, fully able to identify and articulate his/her needs in the required form. Most dimensions of human self-expression include implicit, intangible, subtle and fuzzy forms, making it – at least for the time being – impossible to reconstruct them adequately. In addition, if individual preferences with regard to a specific application or situation tend to change frequently and dynamically, the expediency of user-supported profiling is significantly reduced.

These considerations on profiling are not intended to support the conclusion that profiling is to be dismissed per se. Instead, a better understanding of the innate limits to the construction of user profiles should entail a heightened awareness of the necessity to implement adequate provisions that help to reduce undesirable side-effects. This could, for instance, be achieved by system designs that always enable users to easily overrule decisions made by an AmI system.[168]

### 9.4.2 Loss of control

The problems associated with loss of control can arise from (1) simple annoyances in day-to-day interactions with AmI, (2) uneasiness caused by the lack of transparency of systems operating in the background, (3) unpleasant or even frightening experiences if one is confronted with unexpected system behaviour, and (4) serious intimidations caused by malicious exploitation of technical vulnerabilities. In the first case, the system design did not consider sufficient possibilities for users' control over the system. Failures of this kind originate in inadequate incorporation of user preferences and behavioural patterns in system design. Once more, the general problems with regard to adequate profiling establish natural limits to this remedy. In the second case, the very embeddedness and cloaked nature of many AmI services is accompanied by a lack of transparency. In the third case, the combination of technology dependency and a lack of understanding evoke stress and anger if the system does not behave as expected. And in the fourth case, security measures have been circumvented.

#### *Technology paternalism*

One of the main rationales for creating and implementing AmI systems is to assist in the management of complex processes, which previously had to be accomplished by the user. Thus, the declared objective of the AmI system is to take a certain burden – mostly standardised tasks with frequent repetitions – away from the individual in order to raise the level of convenience, security and/or efficiency. The commonly envisioned application areas of AmI systems are manifold and well known, including the management of environmental parameters such as room temperature, lighting, etc., according to individual preferences; the management of communications according to predefined rules and/or based on machine-learning;[169] and implementing security provisions in mobility situations restricting certain behaviour or informing the user in case of a potential danger.

[168] Spiekermann, S., and F. Pallas, "Technology Paternalism – Wider Implications of Ubiquitous Computing", *Poiesis & Praxis*, Vol. 4, no. 1, 2006, pp. 6-18.
[169] Cf. the above-mentioned difficulties in constructing adequate profiles.

Technology paternalism[170] arises in those instances in which machines decide autonomously and uncontrolled on behalf and in the supposedly best interest of a user. Technology effectively infringes upon individual liberty if no easy-to-use and convenient override options are available and the user does not want to comply with the settings of an AmI system – for whatever reason. The possible drawbacks from technology paternalism can range from constant irritations to fundamental distrust in AmI, possibly leading to the deliberate decision to avoid AmI systems as far as possible.

### *Lack of transparency*

As has been pointed out, one of the central features of many existing and envisioned AmI applications is their ability to operate in the background, largely unnoticed by the user. While this defining characteristic doubtlessly has its merits in terms of usability, convenience and efficiency, it may have adverse effects on users' trust in and acceptance of AmI services. Because users know that AmI systems can operate invisibly, autonomously and unperceived, concerns about system control, the possibly hidden agendas of system operators, and secondary use of collected data may arise. In fact, a recent consumer study dealing with acceptance of RFIDs confirmed that users tend to consider themselves as powerless and helpless and feel that they are being left without real choices due to the loss of control in certain AmI environments.[171]

In conventional technology acceptance models, the willingness to use a technology is typically dependent upon its perceived *usefulness* and its *ease of use*.[172] As many AmI services are envisioned to function autonomously in the background, unwillingness and reluctance to use these systems can hardly be ascribed to complicated usage requirements.[173] In fact, other acceptance criteria need to be added to the equation. Due to the absence of interfaces and direct human-machine interaction opportunities in AmI environments, it stands to reason that (dis)trust plays an even more important function with regard to user acceptance of AmI than is the case for most other technologies. An approach to alleviate concerns about latent operations and data misuse, thus reducing distrust, is to enhance transparency by effectively informing users about system procedures, purposes and responsibilities.

### *Unpredictable or unexpected system behaviour*

The AmI vision promises a natural, intuitive and, therefore, unobtrusive way of human-technology interaction. If such a smooth co-operation cannot be attained, there is a risk that ambient intelligence will cause stress and distrust and, as a consequence, the technology will not generate the acceptance necessary to realise the (societal) benefits it promises.

---

[170] For a detailed discussion of the concept, see Spiekermann, S. and F. Pallas, "Technology Paternalism – Wider Implications of Ubiquitous Computing", *Poiesis & Praxis*, Vol. 4, no. 1, 2006, pp. 6-18.
[171] Spiekermann, S., and M. Rothensee, *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing*, Institut für Wirtschaftsinformatik, Humbold-Universität zu Berlin, 2005, pp. 7-9. http://interval.hu-berlin.de/downloads/rfid/neuste%20forschungsergebnisse/SocioPsychofak.pdf.
[172] Cf. Venkatesh, V., "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model", *Information Systems Research*, 11(4), 2000, pp. 342-365.
[173] Spiekermann, S., and M. Rothensee, *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing*, Institut für Wirtschaftsinformatik, Humbold-Universität zu Berlin, 2005, p. 5. http://interval.hu-berlin.de/downloads/rfid/neuste%20forschungsergebnisse/SocioPsychofak.pdf .

Due to the technology's complexity or the different conception that programmers and users have of the proper use of information systems, users may conclude that they cannot rely on the AmI technology as expected. This is especially true for distributed systems whose behaviour is particularly difficult to predict. The possibilities of formal verification, which would ensure that unwanted system states couldn't occur, are limited in this case.

This is a problem especially for those users who are not familiar with information technology. These users often blame themselves if they do not attain the desired goal and are often too reluctant for a second try because they are afraid of damaging something. Only those groups that are always open-minded towards new technologies will adopt AmI and incorporate it into their daily life in the short term.

As the dependency on such systems increases, the potential harm, which could result from a misjudgement of system behaviour, also rises. Where more is at stake than the result of a few hours' work (as is the case with normal computer use today), the distrust of users will increase accordingly.

### 9.4.3 Denial of service and discrimination in case of inadequate profiles

Other than in the case of inadequate profiling in which the deficiencies are caused by discrepancies between individual preferences and poorly constructed profiles (see above), denial of services and incidents of discrimination originate in procedural rules imposed by service providers – either in their own right or in compliance with regulations established by public authorities. In the first case, the individual preferences are the central point of reference for the AmI system; in the latter case, specified profile characteristics have to be met by the individual if he or she desires access to certain services or privileges. Furthermore, a closer look into the general problem of service denials reveals that a user might not only be turned down because his/her profile does not match the required criteria (e.g., income, age, health record or other aspects of the personal data history). It is conceivable that an individual's deliberate decision not to make available certain elements of personal data will result in exclusion. This raises the two issues of proportionality and of the possibilities of opting out without experiencing undue restraints. Furthermore, the sophisticated issues to what degree information disclosure is actually necessary in order to achieve certain objectives (smoothly functioning services, civil security, etc.), which types of information service providers should not be allowed to ask for and which additional data sources might be used are touched upon.

Situations in which discriminatory refusals of services can take place are characterised by asymmetric relationships in which one party is obliged to comply with standards defined by the other party – though this will be hard to distinguish from the freedom of contract in individual cases. Two main realms of discriminatory practices due to allegedly inadequate profiles can be distinguished: concerns regarding civil security and practices mainly driven by commercial interests.

- **Civil security:** Based on security concerns, users are requested to provide personal information as a prerequisite to gain access. In most cases, certain requirements have been established by public authorities, and private companies (e.g., transport services, airports, etc.) are obliged to implement these regulations. However, in cases of service denial, it is not necessarily clear to the user on which grounds the measure was imposed. Apart from the possibility of a technical error (e.g., faulty database), it is

difficult to discern whether the refusal is based on public regulations or the service provider's own rationale – which draws attention to the second type of discriminatory practice. Other reasons for the refusal of services can either be inadequate interoperability of information systems or, in the case of individuals from less developed regions, the absence of personal profile data.

- **Profit interests:** Apart from pure security motives, market and profit considerations can be at the heart of access rules. For instance, customers might be coerced into making available sensitive personal data if they wish to enjoy certain privileges or services (e.g., special insurance premiums, rebates, etc.). Moreover, if a customer deliberatively decides not to comply for legitimate reasons, a service provider might respond by limiting its own liability. Apart from any legal considerations, it seems quite obvious that users who have experienced being deprived of real consumer choices will not develop pronounced trust in AmI applications.

### 9.4.4 Victimisation

Due to faulty profiling, an innocent individual might erroneously be identified as a criminal, a potential security threat or even a terrorist.[174] Apart from technical problems, the likelihood of mistakenly suspecting a person increases if the objectives of security needs and personal privacy rights are not balanced adequately. Moreover, incomplete and/or de-contextualised profile information may also contribute to the victimisation of citizens.

## 9.5 SECURITY

The traditional taxonomy of security threats distinguishes between three main domains in which threats may appear: confidentiality, integrity and availability.[175] Confidentiality implies protection of information from unauthorised use, integrity implies protection of information from unauthorised modification, and availability implies that the system is capable of providing a service when users expect it. The protection properties all rely on the distinction between authorised and unauthorised entities. Protecting confidentiality, integrity and availability is more difficult in a ubiquitous computing environment than in traditional networks for the following reasons:

- *Possible conflict of interests between communicating entities*. In the past, it has been relatively clear who needs to be protected against whom: for example, system owners and operators need to be protected against external attackers and misbehaving internal users; while protecting users against operators was not considered to be a major issue. Nowadays, it is clear that users may need to be protected against operators, and that different parties can have conflicting interests. An example is the typical conflict between the wish for privacy and the interest in service or co-operation. Thus, the concept of multilateral security has emerged. Multilateral security considers the security

[174] Exactly this situation already occurs today. See, for example, Summers, Deborah, "Bureau admits innocents branded criminals", *The Herald* [Scotland], 22 May 2006: "The Home Office was plunged into yet more controversy yesterday as it emerged nearly 1500 innocent people had been branded criminals because of errors by its Criminal Records Bureau." http://www.theherald.co.uk/politics/62460.html

[175] Stajano, F., and R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", first Security & Privacy supplement to IEEE Computer, April 2002, pp. 22-26.

requirements of different parties and strives to balance these requirements.[176] It also regards all parties as possible attackers and takes into account possible conflicts of interest, negotiating them and enforcing the results of the negotiations.

- *Network convergence* (wireless communication is envisioned to be seamless between different networks of devices, physical objects and smart dust, and between different communication technologies used). This implies that such sensitive operations, such as banking, are frequently performed wirelessly and that during the banking session the user device can switch several times between different wireless networks about which little is known beforehand.[177]
- *Large number of* ad hoc *communications* (communications between nodes which encounter each other more or less unexpectedly). In *ad hoc* communications, it is difficult to distinguish between normal and malicious devices, because little is known beforehand about the nodes in the environment. This implies that it is fairly easy to realise a denial-of-service (DoS) attack (to make the service unavailable) by adding *ad hoc* communicating devices that constantly send messages and ask for replies, thus disturbing normal operations.[178]
- *Small size and autonomous mode of operation of devices*. This makes it fairly easy to steal personal devices and smart dust nodes and to physically attack them (e.g., to destroy or modify the memory).[179]
- *Resource constraints of mobile devices*. Examples are limited battery life (making it easier to arrange DoS attacks by exhausting the battery due to unnecessary communications),[180] processing capabilities (which make it difficult to run sophisticated encryption or pattern recognition algorithms) and limited communication range and broadband.

AmI will require security solutions very different from those of today's systems. ISTAG postulated what it called "a new security paradigm" characterised by "conformable" security in which the degree and nature of security associated with any particular type of action will change over time and circumstance.

ISTAG framed the challenge this way: How can we manage the security associated with the multiple personalities and roles we will adopt in a multiplicity of relationships? ISTAG says any security rules must be simple, user-understandable, user-friendly, intuitively usable, socially acceptable, based on co-operation.

Security threats and vulnerabilities fall into two major groups: (1) malicious and (2) unanticipated system behaviour.

---

[176] Ranneberg, K., "Multilateral Security: A Concept and Examples for Balanced Security", ACM New Security Paradigms Workshop, September 2000, 151-162.

[177] Stajano, F., and J. Crowcroft, "The Butt of the Iceberg: Hidden Security Problems of Ubiquitous Systems", in Basten et al. (eds.), *Ambient Intelligence: Impact on Embedded System Design*, Kluwer, Dordrecht, 2003.

[178] Creese, S., M. Goldsmith and I. Zakiuddin, "Authentication in Pervasive Computing", First International Conference on Security in Pervasive Computing, Boppard, Germany, 12-14 March 2003, pp. 116-129.

[179] Becher, A., Z. Benenson and M. Dornseif, "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks", Third International Conference on Security in Pervasive Computing, York, UK, April 2006, pp. 104-118.

[180] Stajano, F., and R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", first Security & Privacy supplement to IEEE Computer, April 2002, pp. 22-26.

(1) Malicious system behaviour due to external attackers and insiders (authorised, but deceitful), which exploit internal system problems. Malicious system behaviour can be caused by criminals, insurance or trading companies (in order to increase their profit, they might want to acquire, e.g., information on drivers' driving behaviour or to modify user-defined filters in order to promote their own advertisements), by governmental organisations which fight against criminals by widespread surveillance, by employees and curious family members who want to benefit from spying.

Malicious system behaviour can be caused by viruses[181], worms[182], Trojans[183], phishing[184], denial of service attacks[185] or physical tampering.[186]

(2) Unanticipated system behaviour or failure due to inadequate design, e.g., internal complexity and lack of user-friendliness. The main reasons are:

- design problems, such as system use in circumstances not predicted by the system designer; programming errors; insufficient reliability or sources of critical components; poor scalability or performance of chosen communication protocols; inadequate range of wireless transmissions;
- an increase in the number of personal computers and lack of enthusiasm of their owners to invest significant efforts into secure system use (which is understandable: security is not the primary goal of most computer systems);
- lack of user-friendly security methods;
- incompatibility of system hardware components or software versions after a system upgrade (the diversity of possible software configurations and limited testing time make thorough testing of all configurations literally impossible);
- networking of personal devices and objects, including ad-hoc networking;
- economic reasons, such as uncertainty regarding costs of security holes.

All of these threats can lead to:

- disruption of the primary operation of the technical system or even its destruction,
- violation of the physical integrity of the victim's home and property,
- endangering one's health and life,
- assaults against personal dignity and general well-being.

In the following sections, these threats and vulnerabilities are dealt with in greater detail.

### 9.5.1 Threats

[181] A virus is hidden, self-replicating software, that propagates by infecting – i.e., inserting a copy of itself into and becoming part of – another program. A virus cannot run by itself; it requires a host program to be activated

[182] A worm is software that can run independently, can propagate a complete working version of itself onto other hosts in a network, and may consume computer resources destructively

[183] A Trojan is software that appears to perform a useful or desirable function, but actually gains unauthorised access to system resources or tricks a user into executing other malicious logic

[184] Phishing means tricking the user into providing identity or banking data by asking the user to confirm his personal data on a fake website which pretends to be a legitimate site, and often looks exactly like a web page of, for example, a user's bank.

[185] Denial of service (DoS) is the prevention of authorised access to a system resource or the delaying of system operations and functions, e.g., the attacker sends huge number of extra messages to a target service provider

[186] Physical tampering means copying or changing data by physical manipulation of a device, e.g., replacing sensors in a sensor node so that they send wrong values

### *Malware*

Malware – spyware, adware, viruses, Trojans, worms, denial of service attacks – have been unfortunate features of daily life on the Internet and, lately, with advanced mobile phones. Often, malware is aimed at uncovering and exploiting personal and confidential data.

A recent survey by the National Cyber Security Alliance and America Online found that four of five computers connected to the Web have some type of spyware or adware installed on them, with or without the owner's knowledge. A UK survey found in 2004 that computer viruses, misuse of systems, fraud and theft had risen sharply over the previous two years. Two thirds of companies (68 per cent) suffered at least one such incident in the previous year, up from 44 per cent in the 2002 survey and just 24 per cent in 2000. Three quarters of the 1,000 businesses polled – 94 per cent of the larger companies – had a security incident in the last year. The average UK business now has roughly one security incident a month and larger ones around one a week. Security breaches frequently left systems inoperable.[187] And the proliferation of malware continues to get worse: spyware reportedly trebled in 2005 over the previous year.[188]

Most computer users acquire spyware and adware simply by browsing certain Web sites, or agreeing to install games or software programs that come bundled with spyware and adware. Computer users may or may not understand what they are consenting to when they click "OK" to the lengthy, legalistic disclosures that accompany games or videos. But those notices are legal contracts that essentially absolve the adware companies from any liability associated with the use or misuse of their programs.[189]

### *Data mining and networking*

Growing opportunities to make money via computers inevitably increases the number of attempts to acquire personal data. Such opportunities include, first, commercial structures: it helps to know an individual's personal financial situation and personal preferences in order to present him or her an attractive offer. Second, insurance companies might search for personal data in order to impose higher insurance fees on those users whose profiles suggest they are higher risks (e.g., users who often drive at night or who engage in dangerous sports such as skydiving). Both categories of interested organisations might provide financial support to developers of spyware.

Third, increased opportunities to perform a crime remotely via networks (such as phishing or remote control of somebody else's personal belongings) also threaten security.

### *Surveillance*

[187] Leyden, John, "Hackers cost UK.biz billions", *The Register*, 28 April 2004. http://www.theregister.co.uk/2004/04/28/dti_security_survey/

[188] Kelly, Lisa, "Spyware attacks triple in 2005", *Computing*, 12 Jun 2006 http://www.vnunet.com/computing/news/2158112/spyware-attacks-triple-2005. See also Krebs, Brian, "Microsoft Releases Windows Malware Stats", *The Washington Post*, 12 June 2006 http://blog.washingtonpost.com/securityfix/2006/06/microsoft_releases_malware_sta.html

[189] Krebs, Brian, "Invasion of the Computer Snatchers", *The Washington Post*, 19 Feb 2006.

Law enforcement authorities and intelligence agencies' interest in surveillance in order to increase the security of society as a whole (on the assumption that total surveillance can help to decrease number of terrorist acts) might hinder development of anti-spyware tools if they do not receive adequate financial support, or limit usage of such tools by general public. The main problem with security is that security is not a primary goal of computer usage; and security measures are often neglected if they are not user-friendly. Thus, security of personal devices depends on how much governments support research, development and distribution of user-friendly security measures. Governments have the power to increase taxation of anti-spyware products and wiretapping detectors (or even to make them illegal), or to make them free of charge.

#### *Inadequate profiling*

Inadequate profiling may not seem like a security threat at first glance, at least not in the traditional understanding of security flaws as a malfunctioning of or as attacks on computers. However, nowadays the term "security" is often being used in a sense related to the safety of individuals, groups or societies. For the safety of users, inadequate profiling can present a threat if it forces users to attempt to fit into right profile or if it generates false positives. For example, if insurance companies impose higher fees on users whose lifestyle they consider "insecure" (e.g., if their food consumption, driving behaviour or recreational activity do not fit their standards), the users are left with the choice of paying more or changing their behaviour according to the wishes of the insurance companies; and this forced behaviour change might be dangerous for their health and life. For example, refusal from usual food might cause allergy or lack of microelements.

### 9.5.2 Vulnerabilities

#### *Increase in personal use of computers and other devices with limited resources*

In earlier days, computers were not really personal: people were mainly using computers owned by their employers, who took care of computer security, timely updates of hardware and anti-virus software, compatibility of installed applications and so on. In today's world, computers have become personal; modern mobile phones themselves have become quite powerful personal computers. Consequently, the burden of taking care of security of personal computers has shifted towards individual users.

This burden can be a hassle even for those who only have to care about the security of their own computers; the situation becomes worse in the case of mobile devices with limited capabilities. Mobile devices have already replaced desktops in many tasks, and this trend will increase in the AmI future. This increases threats to security because running sophisticated encryption algorithms and communication protocols and multi-tasking are difficult for mobile devices. Additionally, limited battery life carries a danger that the device becomes useless unexpectedly; the small screen size of mobile devices carries a danger that users will miss important information due to an unwillingness to scroll down, and so on.

#### *Lack of user-friendly security measures*

Despite the fact that users must take care of their own security, the security of personal devices has not significantly improved compared to the early days of desktop computers: the main means of user authentication in mobile phones is still a PIN code, and user authentication happens only when the phone is switched on. Besides, proper configuration of security settings requires a certain education (which most users don't have), while updates of software require significant explicit user effort. Even software updates on personal desktops are not user-friendly; the need to restart the computer after every update is a hassle.

Consequently, it is not reasonable to expect that all users will take care of timely updates of their anti-virus software or authenticate themselves to their devices frequently enough, and this might be very dangerous.

### *Networking of personal devices and objects*

The vision of AmI is associated with everything communicating with everything: objects, organisations and personal devices constantly exchange messages. This endangers security significantly because one malicious network node can create problems for other nodes if it constantly broadcasts messages and requires replies. A malicious node can spread viruses or distribute false data. Even if other networking devices have good anti-virus protection and don't get infected by this malicious node; and even if they are able to conclude that the received data are not trustworthy, part of their limited communication and computational capabilities and battery life are wasted anyway.

Additional security problem arise from the inflexible communication range of devices: radio signals from devices and objects located in one home or in one car can easily penetrate walls, so that thieves could detect whether a flat is empty or not, and break into one that is. Another problem is created by the sheer increase of radio communications, which can hinder device operation in some cases.

### *Increase in diversity of hardware and software*

Since more and more versions of hardware and software appear in the market, the problem of compatibility between different hardware components connected together and between different versions of software (running on the same device or during attempts to communicate between different devices) becomes critical. Moreover, that incompatibility can be invisible to the user in the sense that devices still function and communicate, but more slowly or with errors: e.g., incomplete compatibility in communication protocols can lead to distortion of transmitted data without the user's noticing it. Incompatibilities between new anti-virus software and old operational systems can lead to security holes.

### *Uncertainties about costs of software imperfection and improper security*

Security has a cost. As long as market requirements or legal regulations do not force manufacturers to provide products with user-friendly security included, and as long as costs for security problems caused by insecure products are somewhat indeterminate (who knows how to estimate the cost of manually deleting 100 spam e-mails, or recovering from identity theft?), the AmI world will face serious security problems. It is impossible to predict all possible configurations of components that users might install on or connect to their devices and increasing competition between companies producing software and

hardware increases the risk that the testing of devices and software may be insufficient to cope with potential vulnerabilities.

#### *Growing complexity of systems and design problems*

The growing complexity of systems increases both the risk of unpredictable system behaviour and the risk of malicious attacks due to security holes caused by the interaction of components. Interactions between operational systems, ant-virus software and customer applications can hinder the functionality of anti-virus software and increase the risk that virus attacks will succeed. They can also slow down customer applications. The complexity of customer applications can cause unpredictable behaviour if applications are used in situations or ways not predicted by their designers (and designers will not be able to predict everything). Further, the reliability and performance of critical components may be insufficient for the ways in which the components are ultimately used.

### 9.5.3 Disruptions to the primary operation of a technical system

The primary operation of a technical system can be disrupted in many ways. For example, in a health care emergency, it may be necessary to connect a patient's personal device to the hospital network in order to acquire the patient's health care history. In order to interoperate with the hospital's emergency network, the patient's personal device may need to be reconfigured, which in turn could disrupt the operation of the personal device or of the emergency network. If the patient's personal device is contaminated with viruses, they may be transferred to the hospital's AmI system together with the patient's data or to another personal device.

## 9.6 DIGITAL DIVIDE

Apart from the ISTAG scenarios, the digital divide issue has scarcely figured in any AmI-related projects, although the EC has initiated a significant eInclusion programme.

The term "digital divide" was coined by Lloyd Morrisett, the former president of the Markle Foundation, in 1995 to denote the gap, the divide "between those with access to new technologies and those without" [190] or between the information "haves" and "have-nots".

At first glance, the digital divide concept encompasses two basic dimensions: the **global**, between developing and developed societies and the **social**, which relates to the information haves and have-nots even within the same nation. Norris adds another dimension, that of the **democratic** divide, which signifies the difference between those who do, and do not, use digital resources to engage, mobilise and participate in public life.[191]

---

[190] National Telecommunications and Information Administration (NTIA), *Falling through the net: Towards Digital Inclusion. A Report on Americans' Access to Technology Tools*, U.S. Department of Commerce, Economics and Statistics Administration, National Telecommunications and Information Administration, Washington, 2000. http://search.ntia.doc.gov/pdf/fttn00.pdf

[191] Norris, Pippa, *Digital divide: Civic engagement, information poverty, and the Internet worldwide.* Cambridge University Press, Cambridge and New York, 2001.

The advent of new technologies has enabled companies to collect a vast amount of personalised data from current and prospective customers, through purchasing information and surveys. By using special data matching techniques, companies are able to make investment and marketing decisions by targeting certain groups. This means that all organisations are increasingly able to exclude large numbers of people from access to basic services and opportunities by selecting more or less "valuable" customers. Profiling facilitates control of consumer behaviour as well as the construction of consumer identities; the latter inhibits social mobility and contributes to people's exclusion.[192]

Red-lining[193] has triggered a somewhat reverse concern from the one that has been contemplated until now. Information technology can actually be itself an engine of exclusion and people are not only excluded *from* information but *by* information as well.[194]

In the context of our information or digital world, access to ICT has become important and indispensable. Those who do not have access to the new technologies are highly disadvantaged or even excluded. In a world of ambient intelligence where technology is undoubtedly much more pervasive than today, access to and use of it becomes even more important: it will be actually part of our everyday life. In this context, digital divide is a crucial issue for societies and it is important to consider its trend: will AmI technologies contribute to the closing or further widening of the gaps?

In general, it seems that AmI will narrow some gaps while widening existing or creating new ones at the same time. Specifically, in terms of physical access to AmI equipment and infrastructure, this is likely to improve, since AmI applications will form an intrinsic part of our every day lives and at least the basic infrastructure is bound to be forthcoming to the majority of the people. Besides, chances are high that the AmI infrastructure will become cheaper and thus more affordable for larger parts of society (although it could also be argued that the network will be more complex, thus the cost higher for the providers). Furthermore, because of the envisioned user friendliness of AmI technology, the required skills and knowledge for its use will be less than that required today to use mobile phones, personal computers and the Internet, thus enabling more people to use its applications and receive the expected benefits. The majority of people are expected to be at least moderately computer literate, especially given the extent of use of technologies in everyday life.

On the other hand, there will still be a percentage of the population that will not have access to AmI applications and even a greater percentage that will have access only to basic infrastructure and not to more sophisticated equipment, thus excluding them from accessing the full benefits of the AmI environment. Moreover, skills and knowledge remain a limiting factor. In a society with extreme levels of technology pervasiveness, people who do not possess the knowledge or the skills to use AmI to some extent will be more seriously excluded than today. It could be argued that though the divide in terms of

[192] Kruger, Danny, *Access Denied? Preventing Information Exclusion*, Demos, London, 1998.

[193] The term "red-lining" refers to a system developed in the nineteenth century by drawing colour-coded maps of London showing the estimated affluence of the inhabitants in different boroughs and is used to describe the deliberate avoidance of certain large areas by the sellers of insurance (Kruger, 1998). The concept of the 21st century "digital red-lining" is not very far from the 19th century one.

[194] Perri 6 and Ben Jupp, *Divided by information? The "digital divide" and the implications of the new meritocracy*, Demos, London, 2001.

knowledge and skills may narrow, the divide wherever it exists would be far more dramatic and serious in nature. In an AmI environment, profiling is a prerequisite for many applications, which will provide more opportunities for companies and other organisations to target specific groups, excluding and discriminating other people, on the basis of their profiles.

Apart from that, serious concerns exist about the persistence of digital divides with regard to income, education and specific age groups[195], as well as gender and race / ethnicity. Should no measures be taken towards closing these divides, they will continue to exist more or less to the same degree as degree as today. The gender gap should, however, be less pronounced than it is today, assuming that more women become confident enough to use new technologies.

The global dimension of the digital divide between developed and developing countries is likely to remain the same or even grow. As long as the gap between developing and developed nations in general does not close, the digital divide will also widen, especially as new technologies emerge, which the under-developed societies do not have access to or cannot use. In effect, certain regions will most likely face the problem of accumulated digital divides.

### 9.6.1 Dependency

A broad range of threats and vulnerabilities in AmI space relate to the digital divide issue. Amongst the most important ones are different aspects of dependency, exclusion and discrimination.

Two types of dependency are identified: system and user dependency. **Technological dependency** refers to the fact that the proper functioning of a technology or a technological system such as AmI depends on the availability of other technologies of the same or even a previous generation. Due to the ubiquity of AmI, the likelihood of technological dependency will be amplified.

**User dependency** relates to a user's severe irritation, frustration or even panic if a certain technological function or service is temporarily not accessible, not available or does not function properly. In its extreme form, user dependency can display symptoms similar to those of psychological addictions or obsessions.

*Technological dependency: insufficient interoperability*

This vulnerability is caused by technological dependency and has two main aspects: spatial and temporal. The spatial aspect concerns the lack of interoperability between geographical entities. In order for AmI to function across borders, different regions and countries need to use technologies that interoperate. Further harmonisation of standards with varying degrees of geographical scope will be needed (e.g., EU, international). Some countries, however, will not be able to afford to fully comply with the standards created in developed countries. Solutions to overcome the potential divides based on insufficient interoperability need to be envisaged.

[195] Zinnbauer, D. et al, eInclusion Vision and Action: Translating vision into practice, vision paper, IPTS, Seville, 2006.

The temporal aspect refers to the lack of interoperability between different generations of tools and devices. This vulnerability may lead to the categorisation and, consequently, the discrimination of users based on socio-economic status or even because of conflicts of interests and preferences.

*High update and maintenance costs*

The drive towards cost-savings could give a boost to the implementation of AmI, but maintenance and updating could be much more costly than initially expected. Therefore, high costs may lead to the widening of the digital divide within societies, where some people would be able to afford costly maintenance and some would not. It could also become apparent between different countries or nations, since the developed ones could afford these costs whereas the developing or under-developed could not.

*User dependency: Systems take control*

This variant of user dependency is caused by a temporary or even total loss of control over an AmI application (due to inadequate system design, for instance). As a consequence, the user might not receive the expected service from the application.

*"AmI technosis"*

The disruption of social behaviour might be caused by a user's over-reliance and dependency on new means of communication made possible by AmI technologies. In this sense, the user may be or feel excluded.

*Stress*

Severe dependency on technologies may lead to stress. If the technology we have fully integrated into day-to-day routines is not accessible (even temporarily), we will not be able to perform in the usual way. Stress may result from uncertainty as to whether it is possible to re-establish a previous functional state.

*Unsafe usage (due to lack of rules)*

The ubiquitous aspect of AmI technology enables usage on the move, i.e., allowing individuals to use it nearly everywhere, which may sometimes lead to incorrect or unsafe use, either by mistake or even on purpose, with consequences that might not be easily anticipated.

### 9.6.2 Exclusion and discrimination

As stated before, digital divide is often referred to as "information exclusion", where people are excluded from but also by information. In this sense, exclusion and discrimination regarding new technologies are two important aspects of the digital divide, in the context of which certain threats and vulnerabilities may arise, as referenced in the following paragraphs.

*Unequal access*

AmI technology has the potential – due to its foreseen user friendliness and intuitive aspects – to bridge some aspects of the current digital divide. On the other hand, AmI technology could also amplify other aspects of unequal access and use. This threat has technical as well as social and organisational dimensions. There are no guarantees that ambient intelligence services will become public utilities to the benefit of all. There will still be many people with limited or no access to more sophisticated AmI applications, and thus they will be unable to receive any of the envisioned value-added services and the expected benefits of the AmI environment. This is also the case between developing and developed countries.

### *Stigmatisation / profiling*

Because many AmI technologies and devices will need profiling data in order to provide users with the expected and suitable services, profiling data will proliferate within the AmI networks. The misuse of profiling data by companies or other organizations may lead to discrimination of people according to their race, ethnicity or socio-economic status, thus exacerbating exclusion and widening the digital divide. The heavy presence of such data may also make the common origins of stigmatisation (cultural, ethnic, socio-economic) more obvious and even generate new forms of discrimination.

### *Victimisation*

Victimisation as a threat has been introduced and analysed in more detail in the section above on trust. However, with regard to the digital divide, the issue of victimisation or the democratic right not to be treated as a criminal as long as one's guilt is not proven can be of consequence, considering the categorisation and thus discrimination and exclusion of users.

### *Voluntary exclusion*

Voluntary exclusion is another form of exclusion. It is likely that AmI, like any emerging technology, will be adopted gradually and that some people may consistently refuse to adopt it, thus intentionally excluding or dividing themselves from others. This rejection, a refusal to adopt new technologies, is basically caused by users' lack of trust in or sufficient awareness of new technologies and their implications; it is also sometimes referred to as resistance to change, a sort of inertia displayed by a segment of society to the introduction of radical changes, which may in turn lead to social disruption.

# 10 SAFEGUARDS

In the third SWAMI report (*Threats, Vulnerabilities and Safeguards in Ambient Intelligence*), we presented a range of safeguards to address the threats and vulnerabilities associated with the key issues of privacy, identity, security, trust and digital divide. Some of these safeguards already exist (e.g., standards, trust marks, etc.), but need to be strengthened in order deal with the threats and vulnerabilities identified in the same report (as well as the two previous reports).

The multiplicity of threats and vulnerabilities associated with AmI will require a multiplicity of safeguards to respond to the risks and problems posed by the emerging technological systems and their applications.[196] Moreover, in order to adequately address an identified threat or vulnerability, a combination of several safeguards might be needed; in other instances, a single safeguard has the potential to address numerous treats and vulnerabilities.

We have grouped safeguards into three main approaches:
- technological,
- socio-economic,
- legal and regulatory.

## 10.1 TECHNOLOGICAL SAFEGUARDS

The main privacy-protecting principles in network applications are
- anonymity (possibility to use a resource or service without disclosure of user identity),
- pseudonymity (possibility to use a resource or service without disclosure of user identity, but still be accountable for that use),
- unlinkability (possibility to use multiple resources or services without others being able to discover that these resources were used by the same user),
- unobservability (possibility to use a resource or service without others being able to observe that the resource is being used).

The main difference between existing network applications and emerging AmI applications is two-fold: first, in the former case, the user has some understanding of which data about him are collected, and has some means to restrict data collection: e.g., to use a public computer anonymously to access certain web pages; to switch off his mobile phone, to pay cash instead of using web service, etc. In the latter case, with the environment full of numerous invisible sensors (which might include video cameras), it is difficult (if not

[196] Other European projects that have dealt or are dealing with some of the same issues as SWAMI have proposed various safeguards. We have referenced these projects in the first SWAMI deliverable, but among those most relevant are ACIP, Ambient Agoras, AMSD, ARTEMIS, BASIS, BIOVISION, eEPOCH, EUCLID, FIDIS, GUIDE, OZONE, PAMPAS, PAW, PISA, PRIME, PROFIT, PROGRESS, RAPID, WWRF. E-Inclusion projects: COST219; Ambient Assisted Living - Preparation of an Art. 169-initiative (AAL) http://www.vdivde-it.de/aal; Conferences, Workshops, Seminars and Tutorials to Support e-Inclusion (CWST) http://cwst.icchp.org/; European Accessible Information Network (EUAIN) http://www.euain.org/; European Internet Accessibility Observatory (EIAO) http://www.eiao.net/; Ambient Intelligence System of Agents for Knowledge-based and Integrated Services for Mobility Impaired users (ASK-IT) http://www.ask-it.org/; Strengthening eInclusion and eAccessibility across Europe (EINCLUSION@EU) http://www.einclusion-eu.org/

impossible) for users to understand and to control data collection and to achieve unobservability, anonymity and pseudonymity. Intelligent data processing, limiting linkability and implementing strong access control to collected data, seems to be the main ways of protecting privacy in such applications. However, such applications present potential privacy threats anyway if the police, intelligence agencies or family members can search through memory aid data, and if the owner of the memory aid discovers some interesting facts which he has not paid attention to while changing places or talking to people.

A second important difference between network applications and emerging AmI applications is that neither mobile devices nor web usage penetrates through such strong privacy protecting borders as walls (it is rarely 100 per cent certain who sends a request from a particular IP address or uses a mobile device) and the human body, while physiological, video and audio sensors, proposed for AmI applications, will have much stronger capabilities to identify a person and to reveal personal activities and feelings.

Consequently, future AmI applications in smart environments will require stronger safeguards, many of which are not yet fully developed. In our third SWAMI report, we proposed research directions for developing privacy-protecting safeguards in future AmI settings.

User-side identity management research has developed a terminology and interfaces for privacy policies (allowing users to specify how their personal data can be used), and proposed that automatic linkability computation (estimating whether an attacker can link two transactions made by the same user) can help to increase user privacy. Service-side identity management research is concerned with management of obligations (which force a specified privacy policy to be followed), privacy audit (checking that personal data were processed according to the attached privacy policies) and anonymisation of personal data and information retrieval. The conclusion is that privacy audit and management of privacy obligations present many research challenges and open questions.

Privacy/identity projects such as FIDIS, GUIDE and PAMPAS are mainly dealing with privacy protection in network applications and, to some extent, with protecting personal data stored in personal devices from everybody except for the device owner. However, these projects are not concerned with emerging applications and future AmI settings. Meanwhile, the PRIME study on the state of the art in privacy protection in network applications, made in 2005, has pointed out many performance problems and security weaknesses.[197]

Privacy protection research is still new, and most efforts are concentrated on data protection for wired and wireless Internet applications. Even in these domains, full privacy-protecting solutions applicable in real life do not exist yet. There is also ongoing research on protection of data stored in personal devices (mainly by means of encryption), but the limited resources of mobile devices present a challenge. Research on privacy protection in such emerging domains as smart environments and smart cars is in its infancy[198], and only generic guidelines have been developed.

[197] Camenisch, J. (ed.), First Annual Research Report, PRIME Deliverable D16.1, 2005. http://www.prime-project.eu.org/public/prime_products/deliverables/rsch/pub_del_D16.1.a_ec_wp16.1_V1_final.pdf.

[198] Such research is, however, going on. An example is the EC-supported CONNECT project, which aims to implement a privacy management platform within pervasive mobile services, coupling research on semantic

The works of Langheinrich et al. suggest how the fair information practices (listed in current data protection laws) can be applied to AmI applications, and show how difficult it might be to apply them.

Most of the research on privacy protection is concerned with dangers of information disclosure. Other privacy aspects have not received much attention from researchers. For example, the privacy aspect known as "the right to be let alone" is rarely discussed by technology researchers, despite its importance.

***Research on digital divide prevention***

Projects dealing with accessibility for all and e-Inclusion (such as COST219: "Accessibility for all to services and terminals for next generation mobile networks", ASK-IT: "Ambient intelligence system of agents for knowledge-based and integrated services for mobility impaired users") are concerned with standardisation, intuitive user interfaces, personalisation, interfaces to all everyday tools (e.g., domotics[199], home health care, computer accessibility for people with disabilities and elderly people), adaptation of contents to the channel capacity and the user terminal and so on.

Standardisation in the field of information technology (including, for example, biometrics) is an important issue in order to achieve interoperability between different products. However, interoperability even in fairly old technologies (such as fingerprint-based identification) has not yet been achieved.

### 10.1.1 Minimal data collection, transmission and storage

Minimising personal data should be factored into all stages of collection, transmission and storage systems. The goal of the minimal data transmission principle is that data should reveal little about the user even in the event of successful eavesdropping and decryption of transmitted data. Similarly, the principle of minimal data storage requires that thieves don't benefit from stolen databases and decryption of their data. Implementation of anonymity, pseudonymity and unobservability methods helps to minimise system knowledge about users at the stages of data transmission and storage in remote databases, but not in cases involving data collection by and storage in personal devices (which collect and store mainly data of the device owner) or storage of videos.

The main goals of privacy protection during data collection are, first, to prevent linkability between diverse types of data collected about the same user and, second, to prevent surveillance by means of spyware or plugging in additional pieces of hardware transmitting raw data (as occurs in wiretapping). These goals can be achieved by

---

technologies and intelligent agents with wireless communications (including UMTS, Wi-Fi and Wi-Max) and context-sensitive paradigms and multimodal (voice/graphics) interfaces to provide a strong and secure framework to ensure that privacy is a feasible and desirable component of future ambient intelligence applications. The two-year project started in June 2006.
http://cordis.europa.eu/search/index.cfm?fuseaction=proj.simpledocument&PJ_RCN=8292795

[199] Domotics is the application of computer and robot technologies to domestic appliances. Information and communication technologies are expected to provide for more comfort and convenience in and around the home. www.domotics.com/

- careful selection of hardware (so that data are collected and transmitted only in the minimally required quality and quantity to satisfy an application's goals, and there are no easy ways to spy on raw and processed data);
- an increase of software capabilities and intelligence (so that data can be processed in real time); and
- deleting data as soon as the application allows.

In practice, it is difficult to determine what "minimally needed application data" means. Moreover, that data can be acquired by different means.

Software capabilities need to be maximised in order to minimise storage of raw data and avoid storage of data with absolute time stamps. We suggest this safeguard in order to prevent accidental logging of sensitive data, because correlation of different kinds of data by time stamps is fairly straightforward.

These safeguards are presented below in more detail:

- In our opinion, the most privacy threatening are physiological sensors and video cameras. Physiological sensors are privacy-threatening because they penetrate deeply inside the human body and can reveal health data and personal feelings. Video cameras, especially those storing raw video data are privacy-threatening because they violate people's expectations that "nobody can see me if I am hidden behind the wall" and because playback of video data can reveal more details than most people pay attention to in normal life. We suggest that usage of these two groups of devices should be restricted to safety applications until proper artificial intelligence safeguards (see below) are implemented.
- Instead of logging raw data, only data features (data features are a limited set of pre-selected characteristics of data, e.g., frequency and amplitude of oscillations) should be logged. This can be achieved by using either hardware filters or real-time pre-processing of data or a combination of both.
- Time stamping of logged data should be limited by making it relative to other application-related information or by averaging and generalising time-stamping.
- Data should be deleted after an application-dependent time, e.g., when a user buys clothes, all information about the textile, price, designer, etc., should be deleted from the clothes' RFID tag. For applications that require active RFID tags (such as for finding lost objects[200]), the RFID identifier tag should be changed, so that no links between the shop database and personal clothes are left.
- Applications that don't require constant monitoring should switch off automatically after a certain period of user inactivity (for example, video cameras should automatically switch off at the end of a game).
- Anonymous identities, partial identities and pseudonyms should be used wherever possible. Using different identities with the absolute minimum of personal data for each application helps to prevent discovery of links between user identity and personal data and between different actions by the same user.

### 10.1.2 Data and software security

[200] Orr, R. J., R. Raymond, J. Berman and F. Seay, "A System for Finding Frequently Lost Objects in the Home", *Technical Report 99*-24, Graphics, Visualization, and Usability Center, Georgia Tech, 1999.

For the purpose of this section, by security, we imply means of data and software protection from malicious actions (e.g., data theft, modifications of program code, etc.), and not security in a wider sense, which in fact can endanger privacy. For example, surveillance of all people in the country might increase security by making it more difficult for criminals to act, but such surveillance would also violate our privacy.

Data and software protection from malicious actions should be implemented by intrusion prevention and by recovery from its consequences. Intrusion prevention can be active (such as antivirus software, which removes viruses) or passive (such as encryption, which makes it more difficult to understand the contents of stolen data).

At all stages of data collection, storage and transmission, malicious actions should be hindered by countermeasures such as the following:

- *cryptography*;
- *watermarking*: a method to conceal a message in such a way that the very existence of the embedded message is undetectable;
- *anti-virus software and firewalls*;
- *automatic updates of antivirus and firewall software*;
- *self-healing methods for personal devices,* in order to switch to redundant functionalities in the event of suspicious execution delays or spyware detection;
- *detection of changes in hardware configuration*;
- *usage of trusted hardware modules*;
- *secure establishing of ad hoc communications*.

### 10.1.3 Privacy protection in networking (transfer of identity and personal data)

Privacy protection in networking includes providing anonymity, pseudonymity and unobservability whenever possible. When data is transferred over long distances, anonymity, pseudonymity and unobservability can be provided by the following methods: first, methods to prove user authorisation locally and to transmit over the network only a confirmation of authorisation; second, methods of hiding relations between user identity and actions by, e.g., distributing this knowledge over many network nodes. For providing anonymity, it is also necessary to use special communication protocols which do not use device IDs or which hide them. It is also necessary to implement authorisation for accessing the device ID: currently most RFID tags and Bluetooth devices provide their IDs upon any request, no matter who actually asked for the ID. Another problem to solve is that devices can be distinguished by their analogue radio signals, and this can hinder achieving anonymity. Additionally, by analysing radio signals and communication protocols of a personal object, one can estimate the capabilities of embedded hardware and guess whether this is a new and expensive thing or old and inexpensive, which is an undesirable feature.

Unobservability can be, to some extent, implemented also in smart spaces and PANs by limiting the communication range so that signals do not penetrate through the walls of a smart space, or of a car, unlike the current situation when two owners of Bluetooth-enabled phones are aware of each other's presence in neighbouring apartments.

Methods of privacy protection in network applications (mainly long-distance applications) include the following:

- *anonymous credentials* (methods to hide user identity while proving the user's authorisation);
- *a trusted third party*: to preserve the relationships between the user's true identity and his/her pseudonym;
- *zero-knowledge techniques* that allow one to prove the knowledge of something without actually providing the secret;
- *secret sharing schemes*: that allow any subset of participants to reconstruct the message provided that the subset size is larger than a predefined threshold.
- *special communication protocols and networks* such as
  - *onion routing*: messages are sent from one node to another so that each node removes one encryption layer, gets the address of the next node and sends the message there. The next node does the same, and so on until some node decrypts the real user address.
  - *Mix networks and crowds* that hide the relationship between senders and receivers by having many intermediate nodes between them.
- *communication protocols which do not use permanent IDs* of a personal device or object; instead, IDs are assigned only for the current communication session. Communication protocols that provide anonymity at the network layer, as stated in the PRIME deliverable[201], are not suitable for large-scale applications: there is no evaluation on the desired security level, and performance is a hard problem.

### 10.1.4 Authorisation and access control

Proper methods of access control are also needed in AmI applications. Physical access control is required in applications such as border control, airport check-ins and office access. Access control methods are required for logging on to computers and personal devices as well as network applications such as mobile commerce, mobile voting and so on. Reliable authentication should have low error rates *and* strong anti-spoofing protection. Work on anti-spoofing protection of iris and fingerprint recognition is going on, but spoofing is still possible.

We suggest that really reliable authentication should be unobtrusive, continuous (that is, several times during an application-dependent time period) and multimodal. So far, there has been limited research on continuous multimodal access control systems.

Recently, the meaning of the term "access control" has broadened to include checking which software is accessing personal data and how the personal data are processed.

Authentication methods include the following:

#### *Biometrics*

Some experts don't believe that biometrics should be the focus of the security approach in an AmI world, since the identification and authentication of individuals by biometrics will always be approximate, is like publishing passwords, can be spoofed and cannot be revoked after an incident.[202]

[201] Camenish, 2005

[202] See, for example, Engberg, Stephan, "Empowerment and Context Security as the route to Growth and Security", and Pfitzmann, Andreas, "Anonymity, unobservability, pseudonymity and identity management

### *Tokens*

### *Implants*

Implants are small physical devices, embedded into a human body (nowadays they are inserted with a syringe under the skin). Implants are used for identification by unique ID number, and some research aims to add a GPS positioning module in order to detect the user's location at any time.

### *Multimodal fusion*

With multi-modal fusion, identification or authentication is performed by information from several sources, which usually helps to improve recognition rates and anti-spoofing capabilities. Multimodal identification and/or authentication can also be performed by combining data from biometric modalities and non-biometric data.

Methods for reliable unobtrusive authentication (especially for privacy-safe unobtrusive authentication) should be developed.

Unobtrusive authentication should enable greater security because it is more user-friendly. People are not willing to use explicit authentication frequently, which reduces the overall security level, while unobtrusive authentication can be used continuously.

Access control should be context-dependent. Access control to software (data processing methods) is needed for enforcing legal privacy requirements and personal privacy preferences.

User-friendly interfaces are needed for providing awareness and configuring privacy policies. Maintaining privacy is not at the user's focus, so privacy information should not be a burden for a user. The user should easily be able to know and configure the following important settings:

- the purpose of the application goal (e.g., recording a meeting)
- how much autonomy the application has
- the information flow from the user
- the information flow to the user.

Standard concise methods of initial warnings should be used to indicate whether privacy-violating technologies (such as those that record video and audio data, log personal identity data, physiological and health data, etc.) are used by ambient applications.

User-friendly interfaces for fast and easy control over the environment should be able to override previous settings, if needed.

Licensing languages or ways to express legal requirements and user-defined privacy policies should be attached to personal data for the lifetime of their transmission, storage and processing. These would describe what can be done with the data in different contexts

---

requirements for an AmI world". Both papers were presented at the SWAMI Final Conference, Brussels, 21-22 March 2006 and can be found at http://swami.jrc.es.

(e.g., in cases involving the merging of databases), and ensure that the data are really treated according to the attached licence. These methods should also facilitate privacy audits (checking that data processing has been carried out correctly and according to prescribed policies), including instances when the data are already deleted. These methods should be tamper-resistant, similar to watermarking.

### 10.1.5 Generic architecture-related solutions

High-level application design to provide an appropriate level of safeguards for the estimated level of threats can be achieved by proper data protection (e.g., by encryption or by avoiding usage of inexpensive RFID tags which do not have access control to their ID) and by minimising the need for active data protection on the part of the user.

High-level application design should also consider what level of technology control is acceptable and should provide easy ways to override automatic actions. When communication capabilities move closer to the human body (e.g., embedded in clothes, jewellery or watches), and battery life is longer, it will be much more difficult to avoid being captured by ubiquitous sensors. It is an open question how society will adapt to such increasing transparency, but it would be beneficial if the individual were able to make a graceful exit from AmI technologies at his or her discretion.

To summarise, the main points to consider in system design are these:

- Data filtering on personal devices is preferred to data filtering in an untrustworthy environment. Services (e.g., location-based services) should be designed so that personal devices do not have to send queries; instead, services could simply broadcast all available information to devices within a certain range. Such an implementation can require more bandwidth and computing resources, but is safer because it is unknown how many devices are present at a location. Thus, it is more difficult for terrorists to plan an attack in the location where people have gathered.
- Authorisation should be required for accessing not only personal data stored in the device, but also for accessing device ID and other characteristics.
- Good design should enable detection of problems with hardware (e.g., checking whether the replacement of certain components was made by an authorised person). Currently mobile devices and smart dust nodes don't check anything if the battery is removed, and do not check whether hardware changes were made by an authorised person, which makes copying data from external memory and replacement of external memory or sensors relatively easy.
- Personal data should be stored not only encrypted, but also split according to application requirements in such a way that different data parts are not accessible at the same time.
- An increase in the capabilities of personal devices is needed to allow some redundancy (consequently, higher reliability) in implementation and to allow powerful multi-tasking: simultaneous encryption of new data and detection of unusual patterns of device behaviour (e.g., delays due to virus activity). An increase in processing power should also allow more real-time processing of data and reduce the need to store data in raw form.
- Software should be tested by trusted third parties. Currently there are many kinds of platforms for mobile devices, and business requires rapid software development, which prevents thorough testing of security and the privacy-protecting capabilities of personal devices. Moreover, that privacy protection requires extra resources and costs.

- Good design should provide the user with easy ways to override any automatic action, and to return to a stable initial state. For example, if a personalisation application has learned (by coincidence) that the user buys beer every week, and includes beer on every shopping list, it should be easy to return to a previous state in which system did not know that the user likes beer. Another way to solve this problem might be to wait until the system learns that the user does not learn beer. However, this would take longer and be more annoying.
- Good design should avoid implementations with high control levels in applications such as recording audio and images as well as physiological data unless it is strictly necessary for security reasons.
- Means of disconnecting should be provided in such a way that it is not taken as a desire by the user to hide.

### 10.1.6 Artificial intelligence safeguards

To some extent, all software algorithms are examples of artificial intelligence (AI) methods. Machine learning and data mining are traditionally considered to belong to this area. However, AI can be a potential safeguard with very advanced reasoning capabilities. Although AI safeguards are not yet mature solutions, research is actively going on.

Many privacy threats arise because the reasoning capabilities and intelligence of software have not been growing as fast as hardware capabilities (storage and transmission capabilities). Consequently, the development of AI safeguards should be supported as much as possible, especially because they are expected to help protect people from accidental, unintentional privacy violation, such as disturbing a person when he would not want to be, or from recording some private action. For example, a memory aid application could automatically record some background scene revealing personal secrets or a health monitor could accidentally send data to "data hunters" if there are no advanced anti-spyware algorithms running on the user's device. Advanced AI safeguards could also serve as access control and anti-virus protection by catching unusual patterns of data copying or delays in program execution.

We recommend that AmI applications, especially if they have a high control level, should be intelligent enough to:
- detect sensitive data in order to avoid recording or publishing such data;
- adapt to a person's ethics;
- adapt to common sense;
- adapt to different cultures and etiquettes for understanding privacy-protecting requirements;
- summarise intelligently online records;
- interpret intelligently user commands with natural interfaces;
- provide language translation tools capable of translating ambiguous expressions;
- detect unusual patterns of copying and processing of personal data;
- provide an automatic privacy audit, checking traces of data processing, data- or code-altering, etc.

These requirements are not easy to fulfil in full scale in the near future; however, we suggest that it is important to fulfil these requirements as much as possible.

### 10.1.7 Recovery means

It seems probable that data losses and identity theft will continue into the future. However, losses of personal data will be more noticeable in the future because of the growing dependence on AmI applications.

Another problem, which should be solved by technology means, is recovery from loss of or damage to a personal device. If a device is lost, personal data contained in it can be protected from strangers by diverse security measures, such as data encryption and strict access control. However, it is important that the user does not need to spend time customising and training a new device (so that denial of service does not happen). Instead, the new device should itself load user preferences, contacts, favourite music, etc, from some back-up service, like a home server. We suggest that ways be developed to synchronise data in personal devices with a back-up server in a way that is secure and requires minimal effort by the user.

### 10.1.8 Conclusion

We suggest that the most important, but not yet mature technological safeguards are the following:

- communication protocols which either do not require a unique device identifier at all or which require authorisation for accessing the device identifier;
- network configurations that can hide the links between senders and receivers of data;
- improving access control methods by multimodal fusion, context-aware authentication and unobtrusive biometric modalities (especially behavioural biometrics, because it poses a smaller risk of identity theft) and by liveness detection in biometric sensors;
- enforcing legal requirements and personal privacy policies by representing them in machine-readable form and attaching these special expressions to personal data, so that they specify how data processing should be performed, allow a privacy audit and prevent any other way of processing;
- developing fast and intuitive means of detecting privacy threats, informing the user and configuring privacy policies;
- increasing hardware and software capabilities for real-time data processing in order to minimise the lifetime and amount of raw data in a system;
- developing user-friendly means to override any automatic settings in a fast and intuitive way;
- providing ways of disconnecting in such a way that nobody be sure why a user is not connected;
- increasing security by making software updates easier (automatically or semi-automatically, and at a convenient time for the user), detection of unusual patterns, improved encryption;
- increasing software intelligence by developing methods to detect and to hide sensitive data; to understand ethics and etiquette of different cultures; to speak different languages and to understand and translate human speech in many languages, including a capability to communicate with the blind and deaf;
- developing user-friendly means for recovery when security or privacy has been compromised.

## 10.2 SOCIO-ECONOMIC SAFEGUARDS

Co-operation between producers and users of AmI technology in all phases from R&D to deployment is essential to address some of the threats and vulnerabilities posed by AmI. The integration of or at least striking a fair balance between the interests of the public and private sectors will ensure more equity, interoperability and efficiency. Governments, industry associations, civil rights groups and other civil society organisations can play an important role in balancing these interests for the benefit of all affected groups.

### 10.2.1 Standards

Standards form an important safeguard in many domains, not least of which are those relating to privacy and information security. Organisations should be expected to comply with standards, and standards-setting initiatives are generally worthy of support.

While there have been many definitions and analyses of the dimensions of privacy, few of them have become officially accepted at the international level, especially by the International Organization for Standardization. The ISO has at least achieved consensus on four components of privacy, as follows:
**Anonymity** ensures that a subject may use a resource or service without disclosing its user identity.
**Pseudonymity** ensures that a user may use a resource or service without disclosing its identity, but can still be accountable for that use.
**Unlinkability** ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
**Unobservability** ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.[203]

Among the ISO standards relevant to privacy and, in particular, information security are ISO/IEC 15408 on evaluation criteria for IT security and ISO 17799, the Code of practice for information security management.

The ISO has also established a Privacy Technology Study Group (PTSG) under Joint Technical Committee 1 (JTC1) to examine the need for developing a privacy technology standard. This is an important initiative and merits support. Its work and progress should be tracked closely by the EC, Member States, industry and so on.

The ISO published its standard ISO 17799 in 2000, which was updated in July 2005. Since then, an increasing number of organisations worldwide formulate their security management systems according to this standard. It provides a set of recommendations for information security management, focusing on the protection of information as an asset. It adopts a broad perspective that covers most aspects of information systems security.[204]

Among its recommendations for organisational security, ISO 17999 states that "the use of personal or privately owned information processing facilities ... for processing business

[203] ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*, First edition, International Organization for Standardization, Geneva, 1999. The standard is also known as the Common Criteria.
[204] Similar standards and guidelines have also been published by other EU Member States: The British standard BS7799 was the basis for the ISO standard. Another prominent example is the German IT Security Handbook (BSI 1992).

information, may introduce new vulnerabilities and necessary controls should be identified and implemented."[205] By implementing such controls, organisations can, at the same time, achieve a measure of both organisational security and personal data protection.

ISO 17799 acknowledges the importance of legislative requirements, such as legislation on data protection and privacy of personal information and on intellectual property rights, for providing a "good starting point for implementing information security".[206]

ISO 17799 is an important standard, but it could be described more as a framework than a standard addressing specificities of appropriate technologies or how those technologies should function or be used. Also, ISO 17799 was constructed against the backdrop of today's technologies, rather than with AmI in mind. Hence, the adequacy of this standard in an AmI world needs to be considered. Nevertheless, organisations should state to what extent they are compliant with ISO 17799 and/or how they have implemented the standard.

### 10.2.2 Audits

Audit logs may not protect privacy since they are aimed at determining whether a security breach has occurred and, if so, who might have been responsible or, at least, what went wrong. Audit logs could have a deterrent value in protecting privacy and certainly they could be useful in prosecuting those who break into systems without authorisation.

In the highly networked environment of our AmI future, maintaining audit logs will be a much bigger task than now where discrete systems can be audited. Nevertheless, those designing AmI networks should ensure that the networks have features that enable effective audits.

### 10.2.3 Open standards

Apart from the positive effects of open innovations as such, we would support the development of protection software (against viruses, spam, spyware, etc.) under the open source development model. Though open source is no panacea for security problems, there is evidence that open source software can lead to robust and reliable products.

Promoting open systems and open standards at a European level could help to build a more trustworthy system, to mediate between public and private control over networked systems and, therefore, to contribute to security and privacy in AmI.[207]

### 10.2.4 Codes of practice

The OECD has been working on privacy and security issues for many years. It produced its first guidelines more than 25 years ago. Its Guidelines on the Protection of Privacy and

---

[205] ISO/IEC 17799:2005(E), *Information Technology – Security techniques – Code of Practice for Information Security Management*, International Organization for Standardization, Geneva, 2005, p. 11

[206] ISO/IEC 17799:2005, p. ix.

[207] Kravitz, D. W., K.-E. Yeoh and N. So, "Secure Open Systems for Protecting Privacy and Digital Services", in T. Sander (ed.), *Security and Privacy in Digital Rights Management,* ACM CCS-8 Workshop DRM 2001, Philadelphia, 5 Nov 2001, Revised Papers, Springer, Berlin, 2002, pp. 106 – 25; Gehring, R. A., "Software Development, Intellectual Property, and IT Security", *The Journal of Information, Law and Technology*, 1/2003. http://elj.warwick.ac.uk/jilt/03-1/gehring.html.

Transborder Flows of Personal Data[208] were (are) intended to harmonise national privacy legislation. The guidelines were produced in the form of a Recommendation by the Council of the OECD and became applicable in September 1980. The guidelines are still relevant today and may be relevant in an AmI world too, although it has been argued that they may no longer be feasible in an AmI world.[209]

The OECD's more recent Guidelines for the Security of Information Systems and Networks are also an important reference in the context of developing privacy and security safeguards. These guidelines were adopted as a Recommendation of the OECD Council (in July 2002). In December 2005, it published a report on "The Promotion of a Culture of Security for Information Systems and Networks", which it describes as a major information resource on governments' effective efforts to date to foster a shift in culture as called for in the aforementioned Guidelines for the Security of Information Systems and Networks.

In November 2003, the OECD published a 392-page volume entitled *Privacy Online: OECD Guidance on Policy and Practice*, which contains specific policy and practical guidance to assist governments, businesses and individuals in promoting privacy protection online at national and international levels.

In addition to these, the OECD has produced reports on other privacy-related issues including RFIDs, biometrics, spam and authentication.[210]

Sensible advice can also be found in a report published by the US National Academies Press in 2003, which said that to best protect privacy, identifiable information should be collected only when critical to the relationship or transaction that is being authenticated. The individual should consent to the collection, and the minimum amount of identifiable information should be collected and retained. The relevance, accuracy and timeliness of the identifier should be maintained and, when necessary, updated. Restrictions on secondary uses of the identifier are important in order to safeguard the privacy of the individual and to preserve the security of the authentication system. The individual should have clear rights to access information about how data are protected and used by the authentication system and the individual should have the right to challenge, correct, and amend any information related to the identifier or its uses.[211]

Among privacy projects, PRIME has identified a set of privacy principles in the design of identity management architecture.
Principle 1: Design must start from maximum privacy.
Principle 2: Explicit privacy rules govern system usage.
Principle 3: Privacy rules must be enforced, not just stated.
Principle 4: Privacy enforcement must be trustworthy.
Principle 5: Users need easy and intuitive abstractions of privacy.
Principle 6: Privacy needs an integrated approach.

---

[208] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
[209] See _as, Johann, "Privacy in Pervasive Computing Environments – A Contradiction in Terms?", *Technology and Society Magazine*, IEEE, Volume 24, Issue 1, Spring 2005, pp. 24-33.
[210] http://www.oecd.org/department/0,2688,en_2649_34255_1_1_1_1_1,00.html
[211] Kent, Stephen T., and Lynette I. Millett (eds.), *Who Goes There?: Authentication Through the Lens of Privacy*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academies Press, Washington, DC, 2003, Chapter 3.

Principle 7: Privacy must be integrated with applications.[212]

Other guidelines were referenced in the first SWAMI report.

### 10.2.5 Trust marks and trust seals

Trust marks and trust seals can also be useful safeguards because the creation of public credibility is a good way for organisations to alert consumers and other individuals to an organisation's practices and procedures through participation in a program that has an easy-to-recognise symbol or seal.

Trust marks and seals are a form of guarantee provided by an independent organisation that maintains a list of trustworthy companies that have been audited and certified for compliance with some industry-wide accepted or standardised best practice in collecting personal or sensitive data. Once these conditions are met, they are allowed to display a trust seal logo or label that customers can easily recognise.[213]

Such a trust mark must implement mechanisms necessary to maintain objectivity and build legitimacy with consumers. Trust seals and trust marks are, however, voluntary efforts that are not legally binding and an effective enforcement needs carefully designed procedures and the backing of an independent and powerful organisation that has the confidence of all affected parties.

Trust seals and trust marks are often promoted by industry, as opposed to consumer-interest, groups. As a result, concerns exist that consumers' desires for stringent privacy protections may be compromised in the interest of industry's desire for the new currency of information. Moreover, empirical evidence indicates that even some eight years after the introduction of the first trust marks and trust seals in Internet commerce, citizens know little about them and none of the existing seals has reached a high degree of familiarity among customers.[214] Though this does not necessarily mean that trust marks are not an adequate safeguard for improving the security and privacy in the ambient intelligence world, it suggests that voluntary activities like self-regulation have – apart from being well designed – to be complemented by other legally enforceable measures.[215]

### 10.2.6 Reputation systems and trust-enhancing mechanisms

In addition to the general influence of cultural factors and socialisation, trust results from context-specific interaction experiences. As is well documented, computer-mediated interactions are different from conventional face-to-face exchanges due to anonymity, lack of social and cultural clues, 'thin' information, and the uncertainty about the credibility and

---

[212] For more details about each principle, see Sommer, Dieter, Architecture Version 0, PRIME Deliverable D14.2.a, 13 October 2004, pp. 35-6 and pp. 57-58. www.prime-project.eu.org.

[213] Pennington, R., H. D. Wilcox and V. Grover, "The Role of System Trust in Business-to-Consumer Transactions", *Journal of Management Information System*, vol. 20, no. 3, 2004, pp. 197-226; Subirana, B., and M. Bain, *Legal Programming: Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond*, Springer, New York, 2005.

[214] Moores, T., "Do Consumers Understand the Role of Privacy Seals in E-Commerce?", *Communications of the ACM*, Vol. 48, no. 3, 2005, pp. 86-91.

[215] Prins, J. E. J., and M.H.M. Schellekens, "Fighting Untrustworthy Internet Content: In Search of Regulatory Scenarios", *Information Polity*, vol.10, 2005, pp. 129-39.

reliability of the provided information that commonly characterise mediated relationships.[216]

In an attempt to reduce some of the uncertainties associated with online commerce, many websites acting as intermediaries between transaction partners are operating so-called reputation systems. These institutionalised feedback mechanisms are usually based on the disclosure of past transactions rated by the respective partners involved.[217] Giving participants the opportunity to rank their counterparts creates an incentive for rule-abiding behaviour. Thus, reputation systems seek to imitate some of the real-life trust-building and social constraint mechanisms in the context of mediated interactions.

So far, reputation systems have not been developed for AmI services. And it seems clear that institutionalised feedback mechanisms will only be applicable to a subset of future AmI services and systems. Implementing reputation systems only makes sense in those cases in which users have real choices between different suppliers (for instance, with regard to AmI-assisted commercial transactions or information brokers). AmI infrastructures which normally cannot be avoided if one wants to take advantage of a service, need to be safeguarded by other means, such as trust seals, ISO guidelines and regulatory action.

Despite quite encouraging experiences in numerous online arenas, reputation systems are far from perfect. Many reputation systems tend to shift the burden of quality control and assessment from professionals to the – not necessarily entirely informed – individual user. In consequence, particularly sensitive services should not exclusively be controlled by voluntary and market-style feedbacks from customers. Furthermore, reputation systems are vulnerable to manipulation. Pseudonyms can be changed, effectively erasing previous feedback. And the feedback itself need not necessarily be sincere, either due to co-ordinated accumulation of positive feedback, due to negotiations between parties prior to the actual feedback process, because of blackmailing or the fear of retaliation.[218] Last not least, reputation systems can become the target of malicious attacks, just like any net-based system.

An alternative to peer-rating systems are credibility-rating systems based on the assessment of trusted and independent institutions, such as library associations, consumer groups or other professional associations with widely acknowledged expertise within their respective domains. Ratings would be based on systematic assessments along clearly defined quality standards. In effect, these variants of reputation- and credibility-enhancing systems are quite similar to trust marks and trust seals (see previous section). The main difference is that professional rating systems enjoy a greater degree of independence from vested interests. And, other than in the case of peer-rating systems which operate literally

---

[216] For an overview over the vast literature on the topic, cf. Burnett, R. and P.D. Marshall, *Web Theory: An Introduction*, Routledge, London 2002, pp. 45-80.

[217] Resnick, P. and R. Zeckhauser, "Trust Among Strangers in Internet Transactions: Empircal Analysis of eBay's Reputation System", in Michael R. Baye (ed.), *The Economics of the Internet and E-Commerce*, Vol. 11 of Advances in Applied Microeconomics, JAI Press, Amsterdam, 2002, pp. 127-157; Vishwanath, A., "Manifestations of Interpersonal Trust in Online Interaction", *New Media and Society*, Vol. 6 (2), 2004, pp. 224 f.

[218] Resnick, P., R. Zeckhauser, E. Friedman and K. Kuwabara,. "Reputation Systems: Facilitating Trust in Internet Interactions", *Communications of the ACM*, 43(12), 2000, pp. 45-48.
http://www.si.umich.edu/~presnick/papers/cacm00/reputations.pdf (retrieved: 11 April 2006).

for free, the independent professional organisations need to be equipped with adequate resources.

On balance, reputation systems can contribute to trust-building between strangers in mediated short-term relations or between users and suppliers, but they should not be viewed as a universal remedy for the ubiquitous problem of uncertainty and the lack of trust.

### 10.2.7 Service contracts

A possible safeguard is a contract between the service provider and the user that has provisions about privacy rights and the protection of personal data and notification of the user of any processing or transfer of such data to third parties. While this is a possible safeguard, there must be some serious doubt about the negotiating position of the user. It's quite possible the service provider would simply say here are the terms under which I'm willing to provide the service, take it or leave it. Also, from the service provider's point of view, it's unlikely that he would want to conclude separate contracts with every single user.

In a world of ambient intelligence, such a prospect becomes even more unlikely in view of the fact that the "user", the consumer-citizen will be moving through different spaces where there is likely to be a multiplicity of different service providers. It may be that the consumer-citizen would have a digital assistant that would inform him of the terms, including the privacy implications, of using a particular service in a particular environment. If the consumer-citizen did not like the terms, he wouldn't have to use the service.

Consumer associations and other civil society organisations (CSOs) could, however, play a useful role as a mediator between service providers and individual consumers and, more particularly, in forcing the development of service contracts (whether real or implicit) between the service provider and the individual consumer. Consumer organisations could leverage their negotiating position through the use of the media or other means of communication with their members. CSOs could position themselves closer to the industry vanguard represented in platforms such as ARTEMIS by becoming members of such platforms themselves. Within these platforms, CSOs could encourage industry to develop "best practices" in terms of provision of services to consumers.

### 10.2.8 Guidelines for ICT research

Government support for new technologies should be linked more closely to an assessment of technological consequences. On the basis of the far-reaching social effects that ambient intelligence is supposed to have and the high dynamics of the development, there is a clear deficit in this area.[219] Research and development (at least publicly supported R&D) must highlight future opportunities and possible risks to society and introduce them into public discourse. Every research project should commit itself to explore possible risks in terms of privacy, security and trust, develop a strategy to cover problematic issues and involve users in this process as early as possible.

[219] Langheinrich, M., "The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects", Paper presented at the Designing for Privacy Workshop, DC Tales Conference, Santorini, Greece, 2003.

A template for "design guidelines" that are specifically addressing issues of privacy has been developed by the "Ambient Agora" project[220] which has taken into account the fundamental rules by the OECD, notably its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted on 23 September 1980 and the more recent *Guidelines for the Security of Information Systems and Networks*.[221]

### 10.2.9 Public procurement

If the state acts as a buyer of strategically important innovative products and services, it contributes to the creation of the critical demand that enables suppliers to reduce their business risk and realise spill-over effects. Thus, public procurement programs can be used to support the demand for and use of improved products and services in terms of security and privacy or identity protection.

In the procurement of ICT products, emphasis should therefore be given to critical issues such as security and trustworthiness. As in other advanced fields, it will be a major challenge to develop a sustainable procurement policy that can cope with ever-decreasing innovation cycles. The focus should not be on the characteristics of an individual product or component, but on the systems into which components are integrated.

Moreover, it is important to pay attention to the secondary and tertiary impacts resulting from deployment of large technical systems such as ambient intelligence. An evaluation of the indirect impacts is especially recommended for larger (infrastructure) investments and public services.

While public procurement of products and services that are compliant with the EU legal framework and other important guidelines for security, privacy and identity protection is no safeguard on its own, it can be an effective means for the establishment and deployment of standards and improved technological solutions.[222]

### 10.2.10 Accessibility and social inclusion

For the purpose of this study, accessibility was viewed as a key concept helping to promote the social inclusion of all citizens in the information society with the use of AmI technologies. We did not focus on specific groups, people with disabilities and older persons, i.e., people with difficulties in accessing these new technologies and services. In

---

[220] Lahlou, S., and F. Jegou, "European Disappearing Computer Privacy Design Guideslines V1", Ambient Agora Deliverable D15.4, Electricité de France, Clamart, 2003. http://www.ambient-agoras.org/downloads/D15[1].4_-_Privacy_Design_Guidelines.pdf. The guidelines were subsequently and slightly modified and can be found at http://www.rufae.org/privacy. See also Langheinrich, M., "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems", in G. D. Abowd, B. Brumitt and S. A. Shafer (eds.), *Proceedings of the Third International Conference on Ubiquitous Computing* (Ubicomp 2001), Springer-Verlag, Berlin, 2001, pp. 273-91.

[221] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Co-operation and Development, Paris, 2001; *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,* Organisation for Economic Co-operation and Development, Paris, 2002.

[222] See for instance Edler, J., (ed.), "Politikbenchmarking Nachfrageorientierte Innovationspolitik", Progress report No. 99, Office for Technology Assessment at the German Parliament, Berlin, 2006; Molas-Gallart, J., "Government Policies and Complex Product Systems: The Case of Defence Standards and Procurement", *International Journal of Aerospace Management*, vol. 1, no. 3, 2001, pp. 268-80.

this study, accessibility is needed to ensure user control, acceptance and enforceability of policy in a user-friendly manner, with a view to support accessibility and the provision of citizens with real equal rights and opportunities in a world of ambient intelligence.

This point may embrace four safeguards (or principles) relating to:

- equal rights and opportunities
- usability (vs. complexity)
- training
- dependability.

*Equal rights and opportunities*

All citizens should have equal rights to benefit from the new opportunities that AmI technologies will offer. This policy will promote the removal of direct and indirect discrimination, will foster access to services and encourage targeted actions in favour of under-represented groups.

*Usability (vs. complexity of use)*

This point will promote system design according to a user-centric approach (=the concept of "design for all"). The design-for-all concept enables all to use applications (speech technology for the blind, pictures for the deaf). It also means designing in a way that applications are user-friendly and can be used intuitively. In short, industry has to make an effort to simplify the usage of ICT, rather than prospective users being forced to learn how to use otherwise complex ICTs.

Better usability will then support easy learning (i.e., learning by observation), user control and efficiency, thus increasing satisfaction and, consequently, user acceptance.

This safeguard fights directly against user dependency and more particularly against user isolation and stress due to the complexity of new technology, which leads to loss of control.

*Training*

This action will promote education programs on learning how to use new technologies and will increase the user awareness about the different possibilities and choices offered by AmI technologies and devices. This safeguard is useful to deter different facets of user dependency, specially the facets associated with social disruption. User awareness is also important to reduce the voluntary exclusion caused by a misunderstanding on how the technology works.

*Dependability*

This safeguard is essential in order to prevent almost all facets of dependency, system dependency as well as user dependency.

### 10.2.11 Raising public awareness

Consumers need to be educated about the privacy ramifications arising from virtually any transaction in which they are engaged. An education campaign should be targeted at different segments of the population. Targeting school-age children should be included in any such campaign.

Any networked device, particularly those used by consumer-citizens should come with a privacy warning much like the warnings on tobacco products.

When the UK Department of Trade and Industry (DTI) released its 2004 information security review, Stephen Timms, the UK e-Commerce minister, emphasised that everyone has a role to play in protecting information: "Risks are not well managed. We need to dispel the illusion the information security issues are somebody else's problem. It's time to roll up our sleeves."[223]

The OECD shares this point of view. It has said that "all participants in the new information society …need… a greater awareness and understanding of security issues and the need to develop a 'culture of security'."[224] The OECD uses the word "participants", which equates to "stakeholders", and virtually everyone is a participant or stakeholder – governments, businesses, other organisations and individual users. Its guidelines are aimed at promoting a culture of security, raising awareness and fostering greater confidence [=trust] among all participants.

There are various ways of raising awareness, and one of those ways would be to have some contest or competition for the best security or privacy-enhancing product or service of the year. The US government's Department of Homeland Security is sponsoring such competitions,[225] and Europe could usefully draw on their experience to hold similar competitions in Europe.

### 10.2.12 Education

In the same way as the principle that "not everything that you read in the newspapers is true" has long been part of general education, in the ICT age, awareness should generally be raised by organisations that are as close to the citizen as possible and trustworthy (i.e., on the local or regional level, national campaigns maybe co-ordinated by ENISA might help). Questions of privacy, identity and security are, or should be, an integral part of the professional education for computer scientists.

SWAMI agrees with and supports the Commission's recent "invitation" to Member States to "stimulate the development of network and information security programmes as part of higher education curricula".[226]

---

[223] Leyden, John, "Hackers cost UK.biz billions", *The Register*, 28 April 2004. http://www.theregister.co.uk/2004/04/28/dti_security_survey/

[224] *OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security*, OECD, Paris, 2002, p. 7.

[225] Lemos, Robert, "Cybersecurity contests go national", *The Register*, 5 June 2006. http://www.theregister.co.uk/2006/06/05/security_contests/
This article originally appeared at *SecurityFocus*. http://www.securityfocus.com/news/11394

[226] European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006], p. 9 (section 3.3.1). http://ec.europa.eu/information_society/doc/com2006251.pdf

### 10.2.13 Media attention, bad publicity and public opinion

Perhaps one of the best safeguards is public opinion, stoked by stories in the press and the consequent bad publicity given to perceived invasions of privacy by industry and government.

New technologies often raise policy issues, and this is certainly true of ambient intelligence. AmI offers great benefits, but the risk of not adequately addressing public concerns could mean delays in implementing the technologies, a lack of public support for taxpayer-funded research and vociferous protests by privacy protection advocates.

### 10.2.14 Cultural safeguards

Cultural artefacts, such as films and novels, may serve as safeguards against the threats and vulnerabilities posed by advanced technologies, including ambient intelligence. Science fiction in particular often presents a dystopian view of the future where technology is used to manipulate or control people, thus, in so doing, such artefacts raise our awareness and serve as warnings against the abuse of technology. A *New York Times* film critic put it this way: "It has long been axiomatic that speculative science-fiction visions of the future must reflect the anxieties of the present: fears of technology gone awry, of repressive political authority and of the erosion of individuality and human freedom."[227]

An example of a cultural artefact is Stephen Spielberg's 2002 film, *Minority Report*, which depicts a future embedded with ambient intelligence, which serves to convey messages or warnings from the director to his audience. *Minority Report* is by no means unique as a cultural artefact warning about how future technologies are like a double-edged knife that cuts both ways.

## 10.3 LEGAL AND REGULATORY SAFEGUARDS

### 10.3.1 Introduction

The fast emergence of information and communication technologies and the growth of on-line communication, e-commerce and electronic services go beyond the territorial borders of the Member States and have led the European Union to adopt numerous legal instruments such as directives, regulations and conventions on e-commerce, consumer protection, electronic signature, cyber crime, liability, data protection, privacy and electronic communication… and many others. Even the European Charter of Fundamental Rights will play an important role in relation with the networked information society in the EU.

The existing legal framework was extensively discussed in the first SWAMI report and its usefulness and effectiveness were examined in a legal analysis of the dark scenarios in the second SWAMI. These exercises have pointed out that there *are* threats and vulnerabilities

[227] Scott, A. O., "A Future More Nasty, Because It's So Near", Film review of "Code 46", *The New York Times*, 6 Aug 2004.

in ambient intelligence and that we may encounter serious legal problems when applying the existing legal framework to address the intricacies of an AmI environment.

The proposed safeguards should be considered as general policy options, aimed at stimulating discussion between stakeholders and, especially, policy-makers.

### 10.3.2 General recommendations

#### *Law and architecture go together (Recommendation 1)*

Law is only one of the available sets of tools for regulating behaviour, next to social norms, market rules, "code"[228] – the architecture of the technology (e.g., of cyberspace, wireless and wired networks, security design, encryption levels, rights management systems, mobile telephony systems, user interfaces, biometric features, handheld devices, accessibility criteria, etc) and many other tools.

The regulator of ambient intelligence can, for instance, achieve certain aims directly by imposing laws, but also indirectly by, for example, influencing the rules of the market. Regulatory effect can also be achieved by influencing the architecture of a certain environment. The architecture of AmI might well make certain legal rules difficult to enforce (for example, the enforcement of data protection obligations on the Internet or the enforcement of copyright in peer-to-peer networks), and might cause new problems, particularly related to the new environment (spam, dataveillance). On the other hand, the "code" has the potential to regulate by enabling or disabling certain behaviour, while law regulates via the threat of sanction. In other words, software and hardware constituting the "code", and architecture of the digital world, causing particular problems, can be at the same time the instrument to solve them. Regulating through code may have some specific advantages: Law traditionally regulates ex post, by imposing a sanction on those who did not comply with its rules (in the form of civil damages or criminal prosecution). Architecture regulates by putting conditions on one's behaviour, allowing or disallowing doing something, not allowing the possibility to disobey. It regulates ex ante.

Ambient intelligence is particularly built on software code. This code influences how ambient intelligence works, e.g., how the data are processed, but this code itself can be influenced and accompanied by regulation.[229] Thus, the architecture can be a tool of law. This finding is more than elementary. It shows that there is a choice: should the law change because of the "code"? Or should the law change "code" and thus ensure that certain values are protected?

The development of technology represents an enormous challenge for privacy, enabling increasing surveillance and invisible collection of data. A technology that threatens privacy may be balanced by the use of a privacy enhancing technology: the "code", as Lessig claims[230], can be the privacy saviour. Other technologies aim to limit the amount of data

[228] Lessig, Lawrence, "The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 133, 1999, pp. 501-546. See also Brownsword, Roger, "Code, control, and choice. Why East is East and West is West", *Legal Studies*, Vol. 25 No 1, March 2005, pp. 1-21.

[229] Contrary to the long-lasting paradigm, as Lessig writes. Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999, and "Commentaries, The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 113:501, 1999, pp. 501-546

[230] Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

actually collected to the necessary minimum. However, most of the current technologies simply ignore the privacy implications and collect personal data when there is no such need. A shift of the paradigm to privacy-by-design is necessary to effectively protect privacy. Indeed, technology can facilitate privacy friendly verification of individuals via, e.g., anonymous and pseudonymous credentials. Leenes and Koops recognise the potential of these privacy-enhancing technologies (PETs) to enforce data protection law and privacy rules.[231] But they also point at problems regarding the use of such technologies, which are often troublesome in installation and use for most consumers. Moreover, industry is not really interested in implementing privacy-enhancing technology. They see no (economic) reason to do it.

The analysis of Leenes and Koops shows that neither useful technology, nor law is sufficient in itself. Equally important is raising stakeholder awareness, social norms and market rules. All regulatory means should be used and have to be used to respond to problems of the new environment to tackle it effectively. *For the full effectiveness of any regulation, one should always look for the optimal mixture of all accessible means.*[232]

### *Precaution or caution through opacity? (Recommendation 2)*

As the impact and effects of the large-scale introduction of AmI in societies spawn a lot of uncertainties, the careful demarche implied of the precautionary principle, with its information, consultation and participation constraints, might be appropriate. The application of this principle might inspire us in devising legal policy options when, as regards AmI, fundamental choices between opacity tools and transparency tools must be made.[233] Opacity tools proscribe the interference by powerful actors into the individual's autonomy, while transparency tools accept such interfering practices, though under certain conditions which guarantee the control, transparency and accountability of the interfering activity and actors.

*In our opinion, most of the challenges arising in the new AmI environment should be addressed by transparency tools (such as data protection and security measures). Transparency should be the default position, although some prohibitions referring to political balances, ethical reasons or core legal concepts should be considered too.*

Legal scholars don't discuss law in general terms. Their way of thinking always involves an application of the law in concrete or exemplified situations. The legislator will compare concrete examples and situations with the law and will not try to formulate general positions or policies. Thus, the proposed legal framework will not deal with the AmI problems in a general way, but focus on concrete issues, and apply opacity and transparency solutions accordingly.

### *Central lawmaking for AmI is not recommended (Recommendation 3)*

---

[231] Leenes, R., and B.J. Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers & Technology*, Vol. 19, No 3, 2005.

[232] Lessig, L.,"Commentaries, The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 113:501, 1999, pp. 501-546

[233] De Hert, Paul, & Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in Erik Claes, Anthony Duff & Serge Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, pp. 61-104.

Another particularity of legal regulation in cyberspace is the absence of a central legislator. Though our legal analysis is based mostly on European law, we emphasise that not everything is regulated at a European level. Regulation of (electronic) identity cards, for instance, concerns a crucial element in the construction of an AmI environment, but is within the powers of the individual Member States.

Both at European and national level, some decision-making competences have been delegated to independent advisory organs (children's rights commissioners, data protection authorities). Hence, there exist many, what we can call, "little legislators" that adjust in some way the often executive power-origin of legislation: The Article 29 Data Protection Working Party, national children's rights commissioners and international standardisation bodies can and do, for example, draft codes of conduct that constitute often (but not always) the basis for new legislation.

*The SWAMI consortium does not suggest the centralisation of the law-making process. On the contrary, we recommend respect for the diversity and plurality of lawmakers. The solutions produced by the different actors should be taken into consideration and be actively involved in policy discussions. Development of case law should also be closely observed. Consulting concerned citizens and those who represent citizens (including legislators) at the stage of development would increase the legitimacy of new technologies.*

### 10.3.3 Preserving the core of privacy and other human rights

#### *Recommendations regarding privacy*

Privacy aims to ensure no interference in private and individual matters. It offers an instrument to safeguard the opacity of the individual and puts limits to the interference by the powerful actors into the individual's autonomy. Normative in nature, regulatory opacity tools should be distinct from regulatory transparency tools, of which the goal is to control the exercise of power rather than to restrict power.[234]

We observe today that the reasonable expectation of privacy erodes[235] due to emerging new technologies and possibilities for surveillance: it develops into an expectation of being

[234] "'Opacity' designates a zone of non-interference which in our opinion must not be confused with a zone of invisibility: privacy, for instance, does not imply secrecy; it implies the possibility of being oneself openly without interference. Another word might have been "impermeability" which is too strong and does not contrast so nicely with "transparency" as "opacity" does. See Hildebrandt, M., and S. Gutwirth (eds.), *Implications of profiling on democracy and the rule of law*, FIDIS (Future of Identity in the Information Society), Deliverable D7.4, September 2005. http://www.fidis.net. See also De Hert P. & S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2005, pp. 61-104; De Hert P. & S. Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence" in *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Institute for Prospective Technological Studies - Joint Research Centre, Seville, July 2003, pp. 111-162 (ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf) and Gutwirth, S., "De polyfonie van de democratische rechtsstaat" [The polyphony of the democratic constitutional state] in M. Elchardus (ed.), *Wantrouwen en onbehagen* [Distrust and uneasiness], Balans 14, VUBPress, Brussels, 1998, pp.137-193.

[235] See Punie Y., S. Delaitre, I. Maghiros & D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D 2, November 2005, Scenario 1 situation 2, p. 18 and p. 77.

monitored. Should this, however, lead to diminishing the right to privacy? Ambient intelligence may seriously threaten this value, but the need for privacy (e.g., the right to be let alone) will probably remain, be it in another form adapted to new infrastructures (e.g., the right to be left off-line).

The right to privacy in a networked environment could be enforced by any means of protecting the individual against any form of dataveillance.[236] Such means are in line with the data minimisation principle of data protection law, which is a complementary tool to privacy. However, in ambient intelligence where collecting and processing personal data is almost a prerequisite, new tools of opacity such as the right to be left "off-line" (in time –e.g., during certain minutes at work – or in space, e.g., in public bathrooms) could be recognised.

Several instruments of opacity can be identified. We list several examples, and there may be others. Additional opacity recommendations are made in subsequent sections, for example, with regard to biometrics. We observe that there is not necessarily an internal coherence between the examples listed below. The list should be understood as a wish list or a list with suggestions to be consulted freely.

### *Recommendation regarding digital territories*

The concept of a digital territory represents a vision that introduces the notions of space and borders in future digitised everyday life. It could be visualised as a bubble, whose boundaries and transparency depends on the will of its owner. The notion of a digital territory aims for a "better clarification of all kinds of interactions in the future information society. Without digital boundaries, the fundamental notion of privacy or the feeling of *being at home* will not take place in the future information society."[237] The concept of digital territories encompasses the notion of a virtual residence, which can be seen as a virtual representation of the smart home.[238]

The concept of digital territories could provide the individual with a possibility to access to – and stay in – a private digital territory of his own at (any) chosen time and place. This private, digital space could be considered as an extension of the private home. Today, already, people indeed store their personal pictures on distant servers; read their private correspondences online; provide content providers with their watching/consuming behaviour for the purpose of digital rights management; communicate with friends and relatives through instant messengers and Internet telephony services. The "prognosis is that the physical home will evolve to 'node' in the network society, implying that it will become intimately interconnected to the virtual world."[239]

---

[236] "Dataveillance means the systematic monitoring of people's actions or communications through the application of information technology", M. Hansen and H. Krasemann (eds.), *Privacy and Identity Management for Europe - PRIME White Paper - Deliverable 15.1.d.,* 18 July 2005, p. 11 (35 p.), with a reference to Clarke, R., "Information Technology and Dataveillance", *Communications of the ACM*, 31(5), May 1988, pp. 498-512, and re-published in C. Dunlop and R. Kling (eds.), *Controversies in Computing*, Academic Press, 1991 available at http://www.anu.edu/people/Roger.Clarke/DV/CACM88.html;

[237] Beslay, L., and H. Hakala, "Digital Territory: Bubbles", p. 11, draft version available at http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf.

[238] Idem.

[239] De Hert, P. & S. Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence", *l.c.*, p. 159.

The law guarantees neither the establishment nor the protection of an online private space in the same way as the private space in the physical world is protected. Currently, adequate protection is lacking.[240] For example, telecommunication service providers will have to keep communication data at the disposal of law enforcement agencies (data retention law). The retention of communication data relates to mobile and fixed phone data, Internet access, e-mail and e-telephony. Data to be retained includes the place, time, duration and destination of communications. What are the conditions for accessing such data? Is the individual informed when such data are accessed? Does he have the right to be present when such data are examined? Does the inviolability of the home extend to the data that are stored on a distant server? Another example of inadequate protection concerns the increasing access to home activities from a distance, e.g., as a result of the communication data generated by domestic applications that are connected to the Internet. In both examples, there is no physical entrance in the private place.[241]

*To ensure that these virtual private territories become a private domain for the individual, a regulatory framework could be established to prevent unwanted and unnoticed interventions similar to that which currently applies to the inviolability of the home.*

*A set of rules needs to be envisaged to guarantee such protection, amongst them, the procedural safeguards similar to those currently applicable to the protection of our homes against state intervention (e.g., requiring a search warrant). Technical solutions aimed at defending private digital territories against intrusion should be encouraged and, if possible, legally enforced.*[242] *The individual should be empowered with the means to freely decide what kind of information he or she is willing to disclose, and that aspect should be included in the digital territory concept. Similarly, vulnerable home networks should be granted privacy protection. Such protection could be extended to the digital movement of the person, that is, just as the privacy protection afforded the home has been or can be extended to the individual's car, so the protection could be extended to home networks, which might contact external networks*.[243]

### *Recommendation regarding spy-free territories for workers and children*

Privacy at the workplace has already been extensively discussed.[244] Most of the legal challenges that may arise can be answered with legal transparency rules, as discussed

---

[240] Idem. *See also* Beslay, L. & Y. Punie, "The Virtual Residence: Identity, Privacy and Security", *Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview*, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, p. 67. http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html.

[241] See Koops, B.J. & M.M. Prinsen, "Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit" ["Glass house, transparent body. A future view on home law and body integrity"], *Nederland Juristenblad*, 12 March 2005, pp. 624-630.

[242] De Hert, P. & S. Gutwirth, "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence", in *Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview*, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, p. 159.
ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf

[243] Beslay, L., & Y. Punie, "The Virtual Residence: Identity, Privacy and Security", IPTS Report 67. http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html

[244] Punie Y., S. Delaitre, I. Maghiros, & D. Wright, (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D 2, November 2005, paragraph 6.1.1, p. 78. See

above. However, certain more drastic, prohibitive measures may be necessary in certain situations involving too far-reaching or unnecessary surveillance, which a society considers as infringing upon the dignity of the employee. *One of the ways to grant the individual a possibility to escape such disproportional surveillance at the workplace is obliging organisations to create physical spaces at work without surveillance technology, e.g., in social areas where the individual can take a short break and in bathrooms. The idea of cyber territories, accessible to the individual when he is in the workplace, would grant him the possibility of being alone in his private digital or cyber activities.*[245]

In addition, transparency rules are needed to regulate other, less intrusive problems. We recall here the specific role of law-making institutions in the area of labour law. Companies must discuss their surveillance system and its usage in collective negotiations with labour organisations and organisations representing employers before its implementation in a company or a sector, taking into account the specific needs and risks involved (e.g., workers in a bank vs. workers in public administration). *All employees should always be clearly and a priori informed about the employee surveillance policy of the employer (when and where surveillance is taking place, what is the finality, what information is collected, how long it will be stored, what are the (procedural) rights of the employees when personal data are to be used as evidence, etc.).*[246]

Specific cyber territories for children have to be devised along the same lines. The United Nations Convention on the Rights of the Child (1990) contains a specific privacy right for children, and sets up monitoring instruments such as National Children's Rights Commissioners. Opinions of such advisory bodies should be carefully taken into account in policy discussion. National Children's Rights Commissioners could take up problems relating to the permanent digital monitoring of children.

### *Recommendation regarding restrictions on use of illegally obtained evidence*

As pointed out in the first SWAMI report, courts are willing to protect one's privacy but, at the same time, they tend to admit evidence obtained through a violation of privacy or data protection.[247] There is a lack of clarity and uniformity regarding the consequence of privacy violations.

The European Court of Human Rights is unwilling to recognise a right to have evidence obtained through privacy violations rejected.[248] This line of reasoning is followed by at

---

also Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace* (5401/01/EN/Final - WP 55), adopted 29 May 2002, available through http://ec.europa.eu/justice_home/fsj/privacy/.

[245] A similar recommendation has been proposed by the Article 29 Data Protection Working Party in *Working Document on the Processing of Personal Data by means of Video Surveillance* (11750/02/EN - WP 67), adopted 25 November 2002, available through http://ec.europa.eu/justice_home/fsj/privacy/.

[246] Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace* (5401/01/EN/Final - WP 55), adopted 29 May 2002, available through http://ec.europa.eu/justice_home/fsj/privacy/.

[247] Punie Y., S. Delaitre, I. Maghiros & D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D 2, November 2005, paragraph 6.1.1, p. 78.

[248] In fact in the case of *Khan* v. *United Kingdom,* judgement of 12 May 2000, the court rejected the exclusionary rule. In that case, the evidence was secured by the police in a manner incompatible with the requirements of Article 8 of the Convention. The court accepted that the admission of evidence obtained in breach of the privacy right is not necessarily a breach of the required fairness under Article 6 of ECHR (the right to a fair trial), since the process taken as a whole was fair in the sense of Article 6. The evidence against

least some national courts.[249] The fact that there is no general acceptance of an exclusionary rule creates legal uncertainty. Its general acceptance is, however, necessary to protect the opacity of the individual in a more effective way.

*The departure from such position by the courts (namely 'no inclusion of evidence obtained through privacy and/or data protection law infringements') could be considered and legislative prohibition of the admissibility (or general acceptance of the exclusionary rule) of such obtained evidence envisaged*.[250]

### *Recommendations regarding implants*

In ambient intelligence, the use of implants can no longer be considered as a kind of futuristic or extraordinary exception. Whereas it is clear that people may not be forced to use such implants, people may easily become willing to equip themselves with such implants on a (quasi) voluntary basis, be it, for example, to enhance their bodily functions or to obtain a feeling of security through always-on connections to anticipate possible emergency situations. Such a trend requires a careful assessment of the opacity and transparency principles at a national, European and international level.

Currently, in Europe, the issue of medical implants has already been addressed.[251] In AmI, however, implants might be used for non-medical purposes. One of the SWAMI scenarios shows that organisations could force people to have an implant so they could be localised anywhere and any time.

*Now, the law provides for strict safety rules for medical implants. The highest standards of safety should be observed in AmI. The European Group on Ethics in Science and New Technologies also recommends applying the precautionary principle as a legal and ethical principle when it considers the use of implantable technologies. It also reminds us that the principles such as data minimisation, purpose specification, proportionality and relevance are in particular applicable to implants. It means, inter alia, that implants should only be used when the aim cannot be achieved by less body-intrusive means. Informed consent is necessary to legitimise the use of implants. We agree with those findings*.

The European Group on Ethics in Science and New Technologies goes further, stating that non-medical (profit-related) applications of implants constitute a potential threat for human dignity. Applications of implantable surveillance technologies are only permitted when

---

the accused was admitted and led to his conviction. The Khan doctrine (followed in cases such as Doerga v. the Netherlands and P.G. and J.H. v. The United Kingdom) is discussed in De Hert, P., "De soevereiniteit van de mensenrechten: aantasting door de uitlevering en het bewijsrecht" [Sovereignty of human rights: threats created by the law of extradition and by the law of evidence], Panopticon, *Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, Vol. 25, No. 3, 2004, pp. 229-238 and in De Hert P. & F.P. Ölcer, "Het onschadelijk gemaakte Europees privacybegrip. Implicaties voor de Nederlandse strafrechtspleging" [The notion of privacy made innocent. Implications for criminal procedure], *Strafblad. Het nieuwe tijdschrift voor strafrecht,* Vol. 2, No 2, 2004, pp. 115-134. See also De Hert, P., *Biometrics: legal issues and implications,* Background paper for the Institute of Prospective Technological Studies, DG JRC, European Commission, Sevilla, January 2005, p. 33.

[249] Cour de Cassation (Belgium) 2 March 2005, http://www.juridat.be.

[250] Although such a finding seems to contradict current case law (such as the Khan judgement, refusing to apply the principle that illegally obtained privacy evidence should be rejected).

[251] Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active medical devices, *Official Journal* L 323 , 26 November 1997, p. 39

there is an urgent and justified necessity in a democratic society, and must be specified in legislation.[252] We agree that such applications should be diligently scrutinised.

*We propose that the appropriate authorities (e.g., the Data Protection Officer) control and authorise applications of implants after the assessment of the particular circumstances in each case. When an implant enables tracking of people, people should have the possibility to disconnect the implant at any given moment and they should have the possibility to be informed when a (distant) communication (e.g., through RFID) is taking place.*

*We agree with the European Group on Ethics in Science and New Technologies that irreversible ICT implants should not be used, except for medical purposes. Further research on the long-term impact of ICT implants is also recommended.*[253]

### *Recommendations regarding anonymity, pseudonymity, credentials and trusted third parties*

Another safeguard to guarantee the opacity of the individual is the possibility to act under anonymity (or at least under pseudonymity or 'revocable anonymity').

The Article 29 Working Party has considered anonymity as an important safeguard for the right to privacy. We can repeat here its recommendations:
(a) The ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on-line as they currently enjoy off-line.
(b) Anonymity is not appropriate in all circumstances.
(c) Legal restrictions which may be imposed by governments on the right to remain anonymous, or on the technical means of doing so (e.g., availability of encryption products) should always be proportionate and limited to what is necessary to protect a specific public interest in a democratic society.
(d) The sending of e-mail, the passive browsing of world-wide web sites, and the purchase of most goods and services over the Internet should all be possible anonymously.
(e) Some controls over individuals contributing content to on-line public fora are needed, but a requirement for individuals to identify themselves is in many cases disproportionate and impractical. Other solutions are to be preferred.
(f) Anonymous means to access the Internet (e.g., public Internet kiosks, pre-paid access cards) and anonymous means of payment are two essential elements for true on-line anonymity.[254]

According to the Common Criteria for Information Technology Security Evaluation Document (ISO 15408),[255] anonymity is only one of the requirements for the protection of privacy, next to pseudonymity, unlinkability, unobservability, user control/information management and security protection. All these criteria should be considered as safeguards for privacy.

---

[252] European Group on Ethics in Science and New Technologies, "Ethical Aspects of ICT Implants in the Human Body", Opinion to the Commission, 16 March 2005.
http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf
[253] Idem.
[254] Article 29 Data Protection Working Party, *Recommendation 3/97: Anonymity on the Internet* (WP 6), adopted on 3 December 1997, available through http://ec.europa.eu/justice_home/fsj/privacy/.
[255] ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*, First edition, International Organization for Standardization, Geneva, 1999.

The e-signature directive promotes the use of pseudonyms and, at the same time, aims to provide security for transactions. *The probative value of digital signatures is regulated differently under the national laws of Member States*.[256] *More clarity as to the legal value of electronic signatures would be desirable, so that its admissibility as evidence in legal proceedings is fully recognised*.[257] *The status of pseudonymity under the law needs further clarification. A pseudonym prevents disclosure of the real identity of a user, while still enabling him to be held responsible to the other party if necessary. It may provide a privacy tool, and remedy against profiling. Using different pseudonyms also prevents the merging of profiles from different domains. It is, however, unclear what is the legal status of pseudonyms (whether they should be regarded as anonymous data or as personal data falling under the data protection regime). Clarification of the issue is desirable*.[258]

In ambient intelligence, the concept of *unlinkability* can become as important as the concept of anonymity or pseudonymity. Unlinkability "ensures that a user may make multiple uses of resources or services without others being able to link these uses together.... Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system."[259] When people act pseudonymously or anonymously, their behaviour in different times and places in the ambient intelligence network could still be linked and consequently be subject to control, profiling and automated decision-making: linking data relating to the same *non-identifiable* person may result in similar privacy threats as linking data that relate to an identified or identifiable person.

*Thus, in addition to and in line with the right to remain anonymous goes the use of anonymous and pseudonymous credentials, accompanied with unlinkability in certain situations (e.g., e-commerce), reconciling thus the privacy requirements with the accountability requirements of, e.g., e-commerce. In fact, such mechanisms should always be foreseen when disclosing someone's identity or when linking the information is not necessary. Such necessity should not be easily assumed, and in every circumstance more*

---

[256] The German example was described in: Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, p. 29. http://www.fidis.net

[257] Currently the directive on electronic signatures states that only advanced electronic signatures (those based on a qualified certificate and created by a secure signature-creation device) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data and are admissible as evidence in legal proceedings. Member States must ensure that an electronic signature (advanced or not) is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: (a) in electronic form, (b) not based upon a qualified certificate, (c) not based upon a qualified certificate issued by an accredited certification service-provider, or (d) not created by a secure signature creation device.

[258] Olsen T., T. Mahler, et al, "Privacy – Identity Management, Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", LEGAL IST: LEGAL Issues for the Advancement of Information Society Technologies, Deliverable D11, 2005. See LEGAL IST website http://193.72.209.176/default.asp?P=369&obj=P1076

[259] ISO99 ISO IS 15408, 1999. http://www.commoncriteria.org/. See also Pfizmann, A. and M. Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology,* Version v0.27, 20 Feb. 2006. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. Pfizmann and Hansen define unlinkability as follows: "*Unlinkability* of two or more items (e.g., subjects, messages, events, actions, ...) means that within the system (comprising these and possibly other items), from the attacker's perspective, these items are no more and no less related than they are related concerning his a-priori knowledge."

*privacy-friendly technological solutions should be sought.*[260] *However, the use of anonymity should be well balanced. To avoid its misuse, digital anonymity could be further legally regulated, especially stating when it is not appropriate.*[261]

### *Recommendation regarding criminal liability rules*

Provisions on criminal liability are necessary to prevent cybercrime. The criminal law is a basic means to fight hackers, attackers and others tending to abuse the possibilities of communication. Moreover, *effective* criminal provisions have a general deterrent effect, thus stopping people from undertaking criminal activities.

Cybercrime has cross-border dimensions and global implications. The restrictive interpretation of criminal laws ('nulla poena sine crimen') requires international consensus on the definition of the different crimes. This issue has been addressed extensively by the Cybercrime Convention[262], which provides a definition for several criminal offences related to cybercrime and for general principles concerning international co-operation. The Cybercrime Convention, however, allows for different standards of protection. The Convention obliges its signatories to criminalise certain offences under national law, but member states are free to narrow the scope of the definitions. The most important weakness of this Convention is the slow progress in its ratification by signatory states.

Council Framework Decision 2005/222/JHA also provides for criminal sanctions against cybercrimes. The Framework decision is limited, however, both in scope and territory, since it only defines a limited number of crimes and is only applicable to the 25 Member States of the European Union.

*It is highly recommended that governments ensure a proper ratification of the Convention. A "revision" mechanism would desirable so that signatories could negotiate and include in the convention definitions of new, emerging cybercrimes. Specific provisions criminalising identity theft and (some forms of) unsolicited communication could be included within the scope of the Convention.*

International co-operation in preventing, combating and prosecuting criminals is needed and may be facilitated by a wide range of technological means, but these new technological possibilities should not erode the privacy of innocent citizens who are deemed to be not guilty until proven. Cybercrime prosecution, and more importantly crime prevention might be facilitated by a wide range of technological means, among them, those that provide for the security of computer systems and data against attacks.[263]

---

[260] Leenes, Ronald And Bert-Jan. Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, p.37.

[261] Compare Gasson, M., M. Meints and K. Warwick, (eds.), "A study on PKI and biometrics", FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, pp. 35-36. http://www.fidis.net

[262] Council of Europe - Cybercrime Convention of 23 November 2001.

[263] Pfitzmann, A. and M. Kohntopp, "Striking a Balance between Cyber-Crime and Privacy", *IPTS Report* 57, EC-JRC, Seville, Sept 2001. http://www.jrc.es/home/report/english/articles/vol57/welcome.htm

### 10.3.4 Specific recommendations regarding data protection

#### *Introduction*

Almost all human activity in AmI can be reduced to personal data processing: opening doors, sleeping, walking, eating, putting lights on, shopping, walking in a street, driving a car, purchasing, watching television and even breathing. In short, all physical actions become digital information that relates to an identified or identifiable individual.

Often, the ambient intelligence environment will need to adapt to individuals and will therefore use profiles applicable to particular individuals or to individuals within a group profile.[264] AmI will change not only the amount, but also the quality of data collected so that we can be increasingly supported in our daily life (the goal of ambient intelligence). AmI will collect data not only about what we are doing, when we do it and where we are, but also data on how we have experienced things.[265] One can assume that the accuracy of the profiles, on which the personalisation of services depends, will improve as the amount of data collected grows. But as others hold more of our data, so grows the privacy risks. Thus arises the fundamental question: Do we want to minimise personal data collection?

Instead of focusing on reducing the amount of data collected, should we admit that they are indispensable for the operation of AmI, and focus rather on empowering the user with a means to control such processing of personal data?

Data protection is a tool for empowering the individual in relation to the collection and processing of his or her personal data. The European data protection directive imposes obligations on the data controller and supports the rights of the data subject with regard to the transparency and control over the collection and processing of data. It does not provide for prohibitive rules on data processing (except for the processing of sensitive data and the transfer of personal data to third countries that don't ensure an adequate level of protection). Instead, the EU data protection law focuses on a regulatory approach and on channelling, controlling and organising the processing of personal data. As the title of Directive 95/46 indicates, the directive concerns both the protection of the individual with regard to the processing of personal data *and* the free movement of such data. The combination of these two goals in Directive 95/46 reflects the difficulties we encounter in the relations between ambient intelligence and data protection law.

There is no doubt that some checks and balances in using data should be put in place in the overall architecture of the AmI environment. Civil movements and organisations dealing with human rights, privacy or consumer rights, observing and reacting to the acts of states and undertakings might provide such guarantees. It is also important to provide incentives for all actors to adhere to legal rules. Education, media attention, development of good

---

[264] See Hildebrandt, M. and J. Backhouse (eds.), *Descriptive analysis and inventory of profiling practices*, FIDIS (Future of Identity in the Information Society) Deliverable D7.2; Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS Deliverable D7.3. Chapter 7 of this deliverable deals with legal issues on profiling. See also Hildebrandt, M. and S. Gutwirth (eds.), *Implications of profiling on democracy and the rule of law*, FIDIS Deliverable D7.4, September 2005. http://www.fidis.net.

[265] Lahlou, Saadi, Marc Langheinrich and Carsten Rocker, "Privacy and Trust Issues with Invisible Computers", *Communications of the ACM*, Vol. 48 No. 3, March 2005, pp. 59-60.

practices and codes of conducts are of crucial importance. Liability rules and rules aimed at enforcement of data protection obligations will become increasingly important.

### *The right to be informed*

Data protection law provides for the right to information, access or rectification, which constitute important guarantees of individual rights. However, its practical application in an AmI era could easily lead to an administrative nightmare, as information overload would make it unworkable. We should try to remedy such a situation in a way that does not diminish this right.

The individual's right to information is a prerequisite to protect his interests. Such a right corresponds to a decentralised system of identity (data) management, but it seems useful to tackle it separately to emphasise the importance of the individual's having access to information about the processing of his data. Because of the large amounts of data to be processed in an AmI world, the help of or support by intelligent agents to manage such information streams seems indispensable.

*The obligation to inform the data subject about when and which data are collected, by whom and for what purpose gives the data subject the possibility to react to mistakes (and thus to exercise his right to rectification of data) or abuses, and enables him to enforce his right in case of damage. It would be desirable to provide the individual not only with information about what data relating to him are processed, but also what knowledge has been derived from the data*.

Information about what knowledge has been derived from the data could help the individual in proving causality in case of damage. Further research on how to reconcile access to the knowledge in profiles (which might be construed as a trade secret in some circumstances) with intellectual property rights would be desirable.

### *Information notices*

The right to be informed could be facilitated by providing information in a machine-readable language, enabling the data subject to manage the information flow through or with the help of (semi-) autonomous intelligent agents. Of course, this will be more difficult in situations of passive authentication, where no active involvement of the user takes place (e.g., through biometrics and RFIDs).

Thus, information on the identity of the data controller and the purposes of processing could exist both in a human-readable and in a machine-readable language. Although we consider the broad range of information as useful for the data subject and software assistance necessary in the long run, we also recognise the way such information is presented to the user is of crucial importance.
In that respect, the Article 29 Working Party has provided useful guidelines and proposed multi-layer EU information notices[266] essentially consisting of three layers:

[266] Article 29 Data Protection Working Party, *Opinion on More Harmonised Information Provisions* (11987/04/EN - WP 100), adopted on 25 November 2004, available through http://ec.europa.eu/justice_home/fsj/privacy/; Article 29 WP also proposes the examples of such notices (appendixes to the opinion on More Harmonised Information Provisions). See also Meints, M., "AmI – The European Perspective on Data Protection Legislation and Privacy Policies", presentation at the SWAMI

**Layer 1 – The short notice** contains core information required under Article 10 of the Data Protection Directive (identity of the controller, purpose of processing, or any additional information which, in the view of the particular circumstances of the case, must be provided to ensure fair processing). A clear indication must be given as to how the individual can access additional information.

**Layer 2 – The condensed notice** contains all relevant information required under the Data Protection Directive. This includes the name of the company; the purpose of the data processing; the recipients or categories of recipients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the possibility of transfer to third parties, the right to access, to rectify and oppose; choices available to the individual. In addition, a point of contact must be given for questions and information on redress mechanisms either within the company itself or details of the nearest data protection agency.

**Layer 3 – The full notice** includes all national legal requirements and specificities. It could contain a full privacy statement with possible additional links to national contact information.

*We recommend that industry and law enforcement agencies consider this idea, based on the P3P platform, for AmI environments. Electronic versions of such notices should be sufficient in most of circumstances.*

### *Data laundering obligations*

The scenarios in the second SWAMI report highlighted a new kind of practice that has emerged in recent years in the sector of personal data trading: while some companies collect personal data in an illegal way (not informing the data subjects, transferring to third parties without prior consent, usage for different purposes, installing spyware, etc.), these personal data are shared, sold and otherwise transferred throughout a chain of existing and disappearing companies to the extent that the origin of the data and the original data collector cannot be traced back. This practice has been described as "data laundering", with analogy to money laundering: it refers to a set of activities aiming to cover illegitimately the origin of data. In ambient intelligence, the value of personal data and therefore the (illegal) trading in these data will (probably) only but increase.

*A means to prevent data laundering could be creating the obligation for those who buy or otherwise acquire databases, profiles and vast amounts of personal data, to check diligently the legal origin of the data. Without checking the origin and/or legality of the databases and profiles, one could consider the buyer equal to a receiver of stolen goods and thus held liable for illegal data processing. An obligation could be created to notify the national Data Protection Officers when personal data(bases) are acquired. Those involved or assisting in data laundering could be subject to criminal sanctions.*

---

International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006, available at http://swami.jrc.es/pages/deliverables.htm (Report of the final conference).

### *Restricted interoperability*

AmI requires efficient, faultless exchanges of relevant data and information throughout the AmI network. The need for efficiency requires interoperable data formats and interoperable hardware and software for data processing. The first SWAMI scenario about the bus accident has shown the need for interoperability in ambient intelligence. But fully operational generalised interoperable AmI, in which data and data processing technologies are transversally interoperable in all sectors and all applications could threaten trust, privacy, anonymity and security. Full interoperability and free flow of personal data are not always desirable; interoperability should not just be considered as unquestionable.

Interoperability can entail an unlimited availability of personal data for any purpose. Interoperability may infringe upon the finality and purpose specification principles and erode the rights and guarantees offered by privacy and data protection law. Moreover, the purposes for which the data are available are often too broadly described (What is "state security", "terrorism", "a serious crime"?). Data can become available afterwards for *any* purpose. Interoperability of data and data processing mechanisms facilitates possible *function creep* (use of data for purposes other than originally envisaged).

Interoperability could contribute to the criminal use of ambient intelligence, for example, by sending viruses to objects in the network (interoperability opens the door for fast transmission and reproduction of a virus) or abusing data (interoperable data formats make data practical for any usage). Interoperability is thus not only a technological issue.

Awareness – already today – of the possible negative sides of interoperability should bring about a serious assessment of both law and technology *before* the market comes up with tools for interoperability. Legal initiatives in France (e.g., requiring interoperability of the iTunes music platform) and sanctions imposed by the European Commission (imposing interoperability of the Microsoft work group server operating system) indicate clearly that the need for interoperability is desired on a political and societal level.

In the Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 2005,[267] interoperability is defined as the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge". This is, however, a more technological definition: It "explicitly disconnects the technical and the legal/political dimensions from interoperability, assuming that the former are neutral and the latter can come into play later or elsewhere … Indeed, technological developments are not inevitable or neutral, which is *mutatis mutandis* also the case for technical interoperability. The sociology of sciences has shown that any technological artefact has gone through many small and major decisions that have moulded it and given it its actual form. Hence, the development of information technology is the result of micro politics in action. Technologies are thus interwoven with organisation, cultural values, institutions, legal regulation, social imagination, decisions and controversies, and, of course, also the other way round. Any denial of this hybrid nature of technology and society blocks the road

[267] Commission of the European Communities, Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM (2005) 597 final, Brussels, 24 November 2005.

toward a serious political, democratic, collective and legal assessment of technology. This means that technologies cannot be considered as *faits accomplis* or extra-political matters of fact."[268]

This way of proceeding has also been criticised by the European Data Protection Supervisor, according to whom this leads to justifying the ends by the means.[269]

*Taking into account the need for interoperability, restrictions in the use and implementation of interoperability are required, amongst others based on the purpose specification and proportionality principles. To this extent, a distinction between the processing of data for public (enforcement) and private (support) purposes, may be absolutely necessary. Access to the databases by state enforcement agencies may be granted only on a case-by-case basis. Hereby, interoperability should not only be seen as a technical issue (solved by technical means) but also as a political, legal and economical issue (solved by legal, political and economical means). In addition, interoperability of the ambient intelligence system with third country systems that do not offer an adequate level of protection is very questionable.*[270]

To achieve certain purposes, for which access to data has been granted, access to the *medium* carrying the information (e.g., a chip) may be sufficient, for example, when verifying one's identity. There should always be clarity as to what authorities are being granted access to data. In the case of deployment of centralised databases, a list of authorities that have access to the data should be promulgated in an adequate, official, freely and easily accessible publication.[271] Such clarity and transparency would contribute to security and trust, and protect against abuses in the use of databases.

### *Proportionality and purpose limitation principle*

The proportionality and purpose limitation principles are already binding under existing data protection laws. The collection and exchange of data (including interoperability) should be proportional to the goals for which the data have been collected. It will not be easy to elaborate the principles of proportionality and purpose limitation in ambient intelligence; previously collected data may serve for later developed applications or discovered purposes. It often might occur that the creation and utilisation of databases can create additional benefits (which are thus additional purposes), e.g., in the case of profiling. Those other (derived) purposes should, as has been indicated in the opinion of the

---

[268] De Hert, P., & S. Gutwirth, "Interoperability of police databases: an accountable political choice", to be published in *International Review of Law Computers & Technology*, 2006; De Hert, P., "What are the risks and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection',* No. 1. ww.vub.ac.be/LSTS/pub/Dehert/006.pdf

[269] European Data Protection Supervisor (EDPS), *Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability* (COM (2005) 490 final), Brussels, 28 February 2006.
http://www.edps.eu.int/legislation/Opinions_A/06-02-28_Opinion_availability_EN.pdf

[270] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004)835 final) *OJ C* 181/27, 23 July 2005, 13-29, sub 3.13. See also De Hert, P., "What are the risks and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection',* No. 1. www.vub.ac.be/LSTS/pub/Dehert/006.pdf

[271] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM (2004) 835 final, *Official Journal* C 181/27, 23 July 2005, sub 3.7, pp. 13-29.

European Data Protection Supervisor, be treated as independent purposes for which all legal requirements must be fulfilled.[272]

Technical aspects of system operation can have a great impact on the way a system works, and how the proportionality principles and purpose limitation principles are implemented since they can determine, e.g., if the access to the central database is necessary, or whether access to the chip or part of the data is possible and sufficient.

### *Biometrics*

Biometric technology can be a useful tool for authentication and verification, and may even be a privacy-enhancing technology. However, it can also constitute a threat to the fundamental rights and freedoms of the individual. Thus, specific safeguards should be put in place. Biometric safeguards have already been subject of reflection by European data protection authorities: the Article 29 Working Party stated that biometric data are in most cases personal data, so that data protection principles apply to processing of such data. [273]

On the principle of proportionality, the Article 29 Working Party points out that it is not necessary (for the sake of authentication or verification) to store biometric data in central databases, but in the medium (e.g., a card) remaining in the control of the user.[274]

*The creation and use of centralised databases should always be carefully assessed before their deployment, including prior checking by data protection authorities. In any case, all appropriate security measures should be put in place.*

Framing biometrics is more than just deciding between central or local storage. Even storage of biometric data on a smart card should be accompanied by other regulatory measures that take the form of rights for the card-holders (to know what data and functions are on the card; to exclude certain data or information from being written onto the card; to reveal at discretion all or some data from the card; to remove specific data or information from the card).[275]

Biometric data should not be used as unique identifiers, mainly because biometric data still do not have sufficient accuracy.[276] Of course, this might be remedied in the progress of science and technological development. There remains, however, a second objection: using

---

[272] Idem, sub 3.2.

[273] See Article 29 Data Protection Working Party, *Working document on biometrics* (12168/02/EN - WP 80), adopted on 1 August 2003, available through http://ec.europa.eu/justice_home/fsj/privacy/; Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, available through http://www.fidis.net [deliverables].

[274] See also De Hert, P., *Biometrics: legal issues and implications*, Background paper for the Institute of Prospective Technological Studies, EC – JRC, Sevilla, January 2005, p.13. http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf.

[275] Neuwrit, K., *Report on the protection of personal data with regard to the use of smart cards,* Report of Council of Europe (2001), accessible through http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents, quoted by De Hert, P., *Biometrics: legal issues and implications, o.c.,* p. 26.

[276] Institute for Prospective Technological Studies (IPTS), *Biometrics at the frontiers: assessing the impact on Society*, Study commissioned by the LIBE committee of the European Parliament, EC – DG Joint Research Centre, Seville, February 2005. http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf

biometrics as the primary key will offer the possibility of merging different databases, which can open the doors for abuses (function creep).

European advisory bodies have considered the storage of raw data and the use of biometric data as a unique identifier. Generally speaking, since the raw data might contain more information than actually needed for certain finalities (including information not known at the moment of the collection, but revealed afterwards due to progress in science, e.g., health information related to biometric data), it should not be stored.[277] Other examples of opacity rules applied to biometrics might be prohibitions on possible use of "strong" multi-modal biometrics (unless for high security applications)[278] for everyday activities. Codes of conduct can be appropriate tools to further regulate the use of technology in particular sectors.[279]

### *RFIDs*

AmI will depend on profiling as well as authentication and identification technologies. To enable ubiquitous communication between a person and his or her environment, both things and people will have to be traced and tracked. RFID seems to offer the technological means to implement such tracked. Like biometrics, RFID is an enabling technology for real-time monitoring and decision-making. Like biometrics, RFIDs can advance the development of AmI and provide many advantages for users, companies and consumers.[280]

No legislative action seems needed to support this developing technology. Market mechanisms are handling this. There is, however, a risk to the privacy interests of the individual and for a violation of the data protection principles, as CASPIAN and other privacy groups have stated. [281]

RFID use should be in accordance with privacy and data protection regulations. The Article 29 Working Party has already given some guidelines on the application of the principles of EU data protection legislation to RFIDs.[282] It stresses that the data protection principles (purpose limitation principle, data quality principle, conservation principle,

---

[277] European Data Protection Supervisor (EDPS), *Comments on the Communication of the Commission on interoperability of European databases*, 10 March 2006. http://www.edps.eu.int/legislation/Comments/06-03-10_Comments_interoperability_EN.pdf

[278] Biometrics, and especially multimodal biometrics, may increase the security of an application, and thus privacy as well. In its technical safeguards, the SWAMI consortium proposes use of multi-modal fusion of several less-privacy intrusive biometrics (e.g., fat, weight, height, gait, behavioral patterns) for everyday activities such as user-friendly authentication in mobile phones or authentication of car drivers. Such biometrics have low accuracy now, but as it is just emerging, such technology will most likely become more accurate later, and at the same time represent a lower threat to privacy than "strong" biometrics. For high security applications, we recommend a combination of strong multi-modal biometrics with continuous unobtrusive authentication by less strong biometrics, provided that all modalities of the strong biometrics have good anti-spoofing capabilities. Use of biometrics should always be accompanied by adequate PETs.

[279] Article 29 Data Protection Working Party, *Working document on biometrics*.

[280] A description of RFID technologies and of usages can be found in Hildebrandt M. and J. Backhouse (eds.) *Descriptive analysis and inventory of profiling practices*, FIDIS (Future of Identity in the Information Society), Deliverable D7.2, June 2005, http://www.fidis.net.

[281] See e.g. Günther, Oliver and Sarah Spiekermann, "RFID and the Perception of Control: The Consumer's View", *Communications of the ACM*, Vol. 48, No. 9, 2005, pp. 73-76.

[282] Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology* (10107/05/EN - WP 105), 19 January 2005. Available through http://ec.europa.eu/justice_home/fsj/privacy/

etc…) must always be complied with when the RFID technology leads to processing of personal data in the sense of the data protection directive.[283]

As the Article 29 Working Party points out, the consumer should always be informed about the presence of both RFID tags and readers, as well as of the responsible controller, the purpose of the processing, whether data are stored and the means to access and rectify data. Here techniques of (visual) indication of activation would be necessary. The data subject would have to give his consent for using and gathering information for any specific purpose. The data subject should also be informed about what type of data are gathered and whether the data will be used by the third parties.

*In AmI, such rights may create a great burden, both on the data subject, on the responsible data controller and on all data processors. Though adequate, simplified notices about the the data processors' policy would be welcome (e.g., using adequate pictograms or similar means). In our opinion, such information should always be provided to consumers when RFID technology is used, even if the tag does not contain personal data in itself.*[284] The data subject should also be informed how to discard, disable or remove the tag. The right to disable the tag can relate to the consent principle of data protection, since the individual should always have the possibility to withdraw his consent.

*The possibility to disable the tag should at least be present when the consent of the data subject is the sole legal ground of processing the data. Disabling the tag should not lead to any discrimination of the consumer (e.g., in terms of the guarantee conditions).*

Technological and organisational measures (e.g., the design of RFID systems) are of crucial importance in ensuring that the data protection obligations are respected (privacy by design, e.g., by technologically blocking unauthorised access to the data). Thus, availability and compliance with privacy standards are of particular importance.[285]

---

[283] The concept of "personal data" in the context of RFID technology is contested. WP 29 states: In assessing whether the collection of personal data through a specific application of RFID is covered by the data protection Directive, we must determine (a) the extent to which the data processed relates to an individual and, (b) whether such data concerns an individual who is identifiable or identified. Data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated. In assessing whether information concerns an identifiable person, one must apply Recital 26 of the data protection Directive which establishes 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." And further: "Finally, the use of RFID technology to track individual movements which, given the massive data aggregation and computer memory and processing capacity, are if not identified, identifiable, also triggers the application of the data protection Directive", Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, 10107/05/EN WP 105, 19 January 2005, point 4.1.

[284] Still, such information on a tag can be an unique identifier enabling the profiling activities. See Kardasiadou, Z., and Z. Talidou, *Report on Legal Issues of RFID Technology*, LEGAL IST (Legal Issues for the Advancement of Information Society Technologies) Deliverable D15, 2006, p. 16.

[285] Some standards have already been adopted in the RFID domain. The International Organization for Standardization has developed sector-specific standards, as well as more generic standards. Some standards have also been developed by EPCglobal Ltd. (www.epcglobal.org), an industry-driven organisation, creating standards to connect servers containing information relating to items identified by EPC (Electronic Product Code) numbers.

*SWAMI recommends that data protection concerns be reflected in initiatives leading to standardisation of technical specifications. Privacy assessment of each particular RFID application could be a legally binding obligation.*[286]

*Further research on the RFID technology and its privacy implications is recommended.*[287] This research should also aim at determining whether any legislative action is needed to address the specific privacy concerns of RFID technology. Further development of codes of conducts and good practices is also recommended.[288]

### *Data protection and profiling: a natural pair*

Profiling is as old as life, because it is a kind of knowledge that unconsciously or consciously supports the behaviour of living beings, humans not excluded. It might well be that the insight that humans often "intuitively know" something before they "understand" it can be explained by the role profiling spontaneously plays in our minds.

Thus, there is no reason to prohibit automated profiling and data mining concerning individuals with opacity rules. Profiling activities should in principle be ruled by transparency tools, namely, tools that ensure the visibility, controllability and accountability of the profilers and the participation of those concerned. Our principled stance is similar to the one held in data protection: as a rule, the processing of personal data – collection, registration and processing in the strict sense – is not prohibited but submitted to a number of conditions guaranteeing the visibility, controllability and accountability of the data controller and the participation of the data subjects.

Data protection rules apply to profiling techniques (at least in principle).[289] The collection and processing of traces surrounding the individual must be considered as processing of personal data in the sense of existing data protection legislation. Both individual and group profiling are dependent on such collection and processing of data generated by the activities of individuals. And that is precisely why, in legal terms, no profiling is thinkable outside data protection.

---

[286] Borking, J., "RFID Security, Data Protection & Privacy, Health and Safety Issues", presentation made during European Commission Consultation on RFID, Brussels, 17 May 2006.

[287] Such research is now carried out In the framework of the FIDIS programme and will lead to publication of A report on AmI, profiling and RFID (FIDIS Deliverable 7.7).

[288] An example of such (emerging) initiatives is the EPCglobal Ltd. guidelines regarding privacy in RFID technology, http://www.epcglobal.org/public_policy/public_policy_guidelines.html, and CDT (Centre for democracy and technology) Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology**,** Interim Draft, 1 May 2006, http://www.cdt.org/privacy/20060501rfid-best-practices.php. Though these are good examples of the involvement of stakeholders in the discussion, the results are not fully satisfactory. As a compromise between the different actors, the guidelines do not go far enough in protecting the interests of consumers. Sometimes the ambiguous wording of the guidelines (e.g., whether practicable…) may result in giving flexibility to industry to actually interpret the scope of their obligations.

[289] We add "at least in principle" because we are well aware of the huge practical difficulties of effectively enforcing and implementing data protection, more particularly in the field of profiling. See Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS (Future of Identity in the Information Society) Deliverable D7.3, August 2005. http://www.fidis.net. See also Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", to be published in M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen*, forthcoming, Springer Press, 2007. See also discussion on RFID above.

There is an ongoing debate in contemporary legal literature about the applicability of data protection to processing practices with data that is considered anonymous, viz. data that do not allow the identification of a specific individual.[290] This debate also has repercussions on the legal regime on profiling. Some contend that data protection rules do not allow processing practices that bring together data on certain individuals without trying to identify the said individual (in terms of physical location or name). Some contend that data protection rules do not apply to profiling practices that process data relating to non-identifiable persons (in the sense of the data protection directive). We hold that it is possible to interpret the European data protection rules in a broad manner covering *all* profiling practices,[291] but the courts have not spoken on this yet.

*More important in this context is our belief that data protection should apply and that, when confusion in the application and interpretation of the legal instruments remains, they should be adapted as to make this possible. Profiling practices and the consequent personalisation of the ambient intelligence environment lead to an accumulation of power in the hands of those who control the profiles and should therefore be made transparent.*

We are convinced that the principles of data protection are an appropriate starting point to cope with profiling in a democratic constitutional state as they do impose good practices. Nevertheless, while the default position of data protection is transparency ("Yes, you can process, but ..."), it does not exclude opacity rules ("No, you cannot process, unless…"). In relation to profiling, two examples of such rules are relevant. On the one hand, of course, there is the explicit prohibition against making and taking decisions affecting individuals solely on the basis of the automated application of a profile without human intervention (see art. 15 of the data protection directive).[292] This seems obvious because in such situation, probabilistic knowledge is applied to a real person. On the other hand, there is the (quintessential) purpose specification principle, which provides that the processing of personal data must meet specified, explicit and legitimate purposes. As a result, the competence to process is limited to well-defined goals, which implies that the processing of the same data for other incompatible aims is prohibited. Processing of personal data for different purposes should be kept separated. This, of course, substantially restricts the possibility to link different processing and databases for profiling or data mining objectives. The purpose specification principle is definitely at odds with the logics of interoperability and availability of personal data: the latter would imply that all thinkable

[290] We recall that *personal data* in the EU Data Protection Directive refers to "any information relating to an identified or identifiable natural person" (Article 1).

[291] De Hert, P., "European Data Protection and E-Commerce: Trust Enhancing?", in J.E.J. Prins, P.M.A. Ribbers, H.C.A. Van Tilborg, A.F.L. Veth & J.G.L. Van Der Wees (eds.), *Trust in Electronic Commerce*, Kluwer Law International, The Hague, 2002, pp. 190-199. See also Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", l.c.

[292] Article 15. Automated individual decisions. 1. Member States shall grant the right to every person 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. 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

databases can jointly be used for profiling purposes.[293] In other words, the fact that the applicable legal regime to profiling and data mining is data protection does not give a *carte blanche* to mine and compare personal data that were not meant to be connected.[294]

The European Data Protection Supervisor indicated in his Annual Report 2005 a number of processing operations that are likely to encompass specific risks to the rights and freedoms of data subjects, even if the processing does not occur upon sensitive data. This list relates to processing operations (a) of data relating to health and to suspected offences, offences, criminal convictions or security measures (b) intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct (c) allowing linkages, not provided for pursuant to national or Community legislation, between data processed for different purposes (d) for the purpose of excluding individuals from a right, benefit or contract.[295]

### 10.3.5 Specific recommendations regarding security

Software can be the tool for regulating one's behaviour by simply allowing or not allowing certain acts. Thus, technology constituting the "software code" can affect the architecture of the Internet (and thus potentially of AmI) and can provide effective means for enforcing the privacy of the individual. For example, cryptology might give many benefits: it could be used for pseudonymisation (e.g., encrypting IP addresses) and ensuring confidentiality of communication or commerce.[296]

*Privacy-enhancing technologies can have an important role to play, but they need an adequate legal framework.*

The directive on the legal protection of software[297] obliges Member States to provide appropriate remedies against a person committing any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical devices which may have been applied to protect a computer program. This mechanism aims to protect programs enforcing the intellectual property rights against circumvention.

*Similar legal protection against circumvention of privacy-enhancing technologies could be legally foreseen.*

Technology might go beyond what the law permits (for example, DRM prevents intellectual property infringements but at the same time might limit the rights of the lawful user). Negative side effects of such technologies should be eliminated. More generally,

---

[293] De Hert, P., "What are the risks and what guarantees need to be put in place in view of interoperability of police databases?", Standard Briefing Note 'JHA & Data Protection', No. 1, produced in January 2006 on behalf of the European Parliament, available through http://www.vub.ac.be/LSTS/

[294] Gutwirth, S. & P. De Hert, "Regulating profiling in a democratic constitutional state", to be published in M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen*, forthcoming, Springer Press, Berlin, 2007.

[295] European Data Protection Supervisor (EDPS), *Annual Report 2005*, pp. 22-23. http://www.edps.eu.int/publications/annual_report_en.htm.

[296] Leenes, Ronald and Bert-Jan Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, pp. 331-332

[297] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17/05/1991, pp. 0042 – 0046.

when introducing new technology on the market, manufacturers together with relevant stakeholders should undertake a privacy impact assessment. *Development of a participatory impact assessment procedure would allow stakeholders to quickly identify and react to any negative features of technology* (see below, where DRMs and intellectual property rights are discussed).

### *Empowering the individual*

The European data protection directive imposes obligations on the data controller and gives rights to the data subject. It aims to give the individual control over the collection and processing of his data. Many provisions in the data protection directive have several weaknesses in an AmI environment. Principles of proportionality and fairness are relative and may lead to different assessments in similar situations; obtaining consent might be not feasible in the constant need for the collection and exchange of data; obtaining consent can be simply imposed by the stronger party. Individuals might not be able to exercise the right to consent, right to information, access or rectification of data due to the overflow of information. Thus, those rules might simply become unworkable in AmI. And even if workable (e.g., thanks to the help of the digital assistants), are they enough? Should we not try to look for an approach granting the individual even more control? Several projects have already considered such an approach and proposed decentralised identity and personal data management and the granting of property over personal information.

### *Decentralised identity (data) management*

Several European projects are involved in research on identity management. They focus on the decentralised approach, where a user controls how much and what kind of information he or she wants to disclose. Identity management systems, while operating on a need-to-know basis, offer the user the possibility of acting under pseudonyms, under unlinkability or anonymously, if possible and desirable.

Among the other examples of such systems,[298] there are projects that base their logic on the assumption that the individual has the property over his data, and then use licensing schemes when a transfer of data occurs. Granting him property over the data[299] is seen as giving him control over the information and its usage in a "distribution chain". However, it is doubtful if in reality granting him property over the data will really empower the individual and give him a higher level of protection and control over his data. The property model also assumes that the data are disseminated under a contract. Thus, the question might arise whether the data protection directive should serve as a minimum standard and

[298] An overview of the existing identity management systems has been given by Bauer M., M. Meints and M. Hansen (eds.), *Structured Overview on Prototypes and Concepts of Identity Management Systems*, FIDIS (Future of Identity in the Information Society) Deliverable D3.1, September 2005, and Hildebrandt M. and J. Backhouse (eds.), *Descriptive analysis and inventory of profiling practices*, FIDIS Deliverable D7.2, June 2005, and Müller G. and S. Wohlgemuth (eds.), *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, May 2005. http://www.fidis.net

[299] See Lessig, L., *Code and other law of cyberspace*, Basic Books, New York, 1999, and Leenes, Ronald, and Bert-Jan Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, pp. 329. See also Samuelson, P., "Privacy As Intellectual Property?", *Stanford Law Review*, Vol. 52, 2000.

thus limit the freedom of contracts.[300] But as the SWAMI dark scenarios show, there exist many cases in which the individual will not be able to *freely* enter into a contract. Another question arises since *our* data are not always collected and used for commercial purposes. Even more, in most situations, the processing of personal data is a necessary condition for entering into a contractual relation (whereas the data protection directive states in Article 7 that data processing without the individual's consent to use of his personal data is legitimate when such processing is necessary for the performance of a contract). The most obvious example is the collection of data by police, social insurance and other public institutions. The individual will not always be free to give or not give his data away. The property model will not address these issues. It will also not stop the availability of the data via public means.[301]

A weakness of the property model is that it might lead to treating data only as economic assets, subject to the rules of the market. But the model's aim is different: the aim is to protect personal data, without making their processing and transfer impossible. Regarding data as property also does not address the issue of the profile knowledge derived from personal data. This knowledge is still the property of the owner or the licenser of the profile. The data-as-property option also ignores the new and increasingly invisible means of data collection, such as RFIDs, cameras or on-line data collection methods.

Discussing the issue of whether personal data should become the individual's property does not solve the core problem. On the one hand, treating data as property may lead to a too high level of protection of personal information, which would conflict with the extensive processing needs of AmI. On the other hand, it would, by default, turn personal data into a freely negotiable asset, no longer ruled by data protection, but left to market mechanisms and consent of the data subjects (more often than not to the detriment of the latter). Finally, the data-as-property option loses its relevance in the light of a focus upon anonymisation and pseudonymisation of data processed in AmI applications.

The PRIME consortium proposes identity management systems controlled by data subjects.[302] It aims to enable individuals to negotiate with service providers the disclosure of personal data according to the conditions defined. Such agreement would constitute a contract.[303] An intelligent agent could undertake the management on the user side. This solution is based on the data minimisation principle and on the current state of legislation. It proposes the enforcement of (some) current data protection and privacy laws. It seems to be more designed for the needs of the world today than for the future AmI. The user could still be forced to disclose more information than he or she wishes, because he or she is the weaker party in the negotiation; he or she needs the service.

The FIDIS consortium also proposed a preliminary vision of decentralised identity management. This vision seems to go a bit further than the PRIME proposal. It foresees that the user profiles are stored with the device of a user, and preferences relevant for a particular service are (temporarily) communicated to the service provider for the purpose

[300] However, currently this is not the case. The weaker party in the contract is now protected by the general principles of law. Prins, J.E.J., "The Propertization of Personal Data and Identities", *Electronic Journal of Comparative Law*, vol. 8.3, October 2004. http://www.ejcl.org/
[301] Idem.
[302] Hansen, Marit and Henry Krasemann (eds.), *Privacy and Identity Management for Europe*, PRIME White Paper, Deliverable D 15.1.d, 18 July 2005. Available through http://www.prime-project.eu.org/.
[303] Ibid., p. 7.

of a single service. The communication of the profile does not have to imply disclosure of one's identity. If there is information extracted from the behaviour of the user, it is transferred by the ambient intelligent device back to the user, thus updating his profile.[304] Thus, some level of exchange of knowledge is foreseen in this model, which can be very important for the data subject's right to information.

*A legal framework for such sharing of the knowledge (from an AmI-generated profile) needs to be developed, as well as legal protection of the technical solution enabling such information management. Such schemes rely on automated protocols for the policy negotiations. The automated schemes imply that the consent of the data subject is also organised by automatic means. It is desirable to clearly foresee a legal framework dealing with the situation wherein the explicit consent of the data subject for each collection of data is replaced by a "consent" given by an intelligent agents.*

In such automated models, privacy policies following the data might also be envisaged. Such "sticky" policies, attached to personal data, would provide for clear information and indication towards data processors and controllers which privacy policy applies to the data concerned.[305] They could facilitate the auditing and self-auditing of the lawfulness of the data processing by data controllers.[306] *In any event, research in this direction is desirable.*

*Since AmI is also a mobile environment, there is a need to develop identity management systems addressing the special requirements of mobile networks.* The FIDIS consortium has done research on the subject and prepared a technical survey of mobile identity management. It has identified some special challenges and threats to privacy in the case of mobile networks and made certain recommendations:

- Location information and device characteristics both should be protected.
- Ease of use of the mobile identity management tools and simplified languages and interfaces for non-experts should be enhanced.
- A verifiable link between the user and his digital identity has to be ensured. Accordingly, privacy should also be protected in peer-to-peer relationships.[307]

### 10.3.6 Specific recommendations regarding consumer protection law

The importance of consumer protection will grow in ambient intelligence, because of the likelihood that consumers will become more dependent on on-line products and services, and because product and service providers will strengthen their bargaining position through an increasing information asymmetry. Without the constraints of law, ambient intelligence service providers easily obtain a position to dictate the conditions of

[304] Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS (Future of Identity in the Information Society) Deliverable D7.3, August 2005, p. 32. http://www.fidis.net.

[305] Meints, M., "AmI - The European Perspective on Data Protection Legislation and Privacy Policies", Presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006.

[306] For example, such an approach was adopted by the PAW project (Privacy in an Ambient World), which has developed the language enabling the distribution of the data in a decentralised architecture, with the usage policies attached to the data, informing what kind of usage has been licensed to the particular actor (licensee). Enforcement relies on auditing. http://www.cs.ru.nl/paw/results.html

[307] Müller G. and S. Wohlgemuth (eds.), *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, May 2005. http://www.fidis.net.

participation in new environments. Consumer protection should find the proper balance in AmI.

Consumer protection law defines the obligations of the producers and the rights of consumer and consists of a set of rules limiting the freedom to contract, for the benefit of the consumer. Consumer protection law plays a role of its own, but can support the protection of privacy and data protection rights.[308]

The basis for the European framework for consumer protection rules can be found in Article 153 of the EC Treaty: "In order to promote the interests of consumers and to ensure a high level of consumer protection, the community shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests."

Consumer protection at European level is provided by (amongst others) Directive 93/13 on unfair terms in consumer contracts[309] and Directive 97/7 on consumer protection in respect of distance contracts[310], and product directives (discussed below). Directive 93/13 and Directive 97/7 were both extensively discussed in the previous SWAMI reports.[311] In many respects, those rules are not fitted to AmI and they need to be re-adapted. This especially relates to extending the scope of protection of those directives, thereby making sure that all services and electronic means of communications and trading are covered (including those services on the World Wide Web not currently covered by the distance selling directive).[312]

### *Contracts could be concluded by intelligent agents*

*Due to the increasing complexity of on-line services, and due to the possibility of information overflow, it seems necessary to find legal ways to assess and recognise contracts made through the intervention of intelligent agents. Is the legal system flexible enough to endorse this? Moreover, the same should apply to the privacy policies and to the consent of individuals for the collection of data (because, in identity management systems, intelligent agents will decide what data are to be disclosed to whom).*

Here is a challenge: how to technologically implement negotiability of contracts and the framework of binding law in electronic, machine-readable form?

### *Unfair privacy policies*

*Suppliers should not be allowed to set up privacy conditions which are manifestly not in compliance with the generally applicable privacy rules and which disadvantage the customer.*

---

[308] Although we focus here on the issue of the services, in an AmI environment, it can be difficult to distinguish between a product and a service. Though it is often difficult to draw the line between the two, different legal regimes apply. Product liability issues are discussed below.

[309] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *Official Journal* L 095, 21/04/1993, pp. 29 – 34.

[310] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *Official Journal* L 144, 04/06/1997, pp. 0019 – 0027.

[311] Friedewald M., E. Vildjiounatie and D. Wright (eds.), *The brave new world of ambient intelligence: A state-of-the-art review,* SWAMI Deliverable D 1, July 2005, p.156.

[312] Henderson, K., and A. Poulter, "The Distance Selling Directive: Points for Further Revision", *International Review for Law Computers & Technology*, Vol. 16 no. 3, 2002, pp. 289-300.

Data protection legislation and consumer protection law could constitute the minimum (or default) privacy protection level. Similar rules as those currently applicable under the consumer protection of Directive 93/13 on unfair terms in consumer contracts could apply. Mandatory rules of consumer protection require, *inter alia,* that contracts be drafted in plain, intelligible language; that the consumer be given an opportunity to examine all terms; that – in case of doubt – the interpretation most favourable to the consumer prevail.

*Suppliers should not be allowed to unfairly limit their liability for security problems in the service they provide to the consumer.*

In this respect, more attention could be given to a judgment of the Court of First Instance of Nanterre (France) in 2004 in which the online subscriber contract of AOL France was declared illegal in that it contained not less than 31 abusive clauses in its standard contractual terms (many of which infringed consumer protection law).[313]

### *Information to the consumer*

The directive on unfair terms in consumer contracts and the directive on consumer protection in respect of distance contracts provide a broad right to information for the consumer. *It should be sufficient to dispense such information in electronic form*[314], in view of the large amount of information directed towards consumers that would have to be managed by intelligent agents.

*An increasing number of service providers will be involved in AmI services and it cannot be feasible to provide the required information about all of them. The solution may be to provide such information only about the service provider whom the consumer directly pays and who is responsible towards the consumer (joint liability would apply; for liability issues, see below).*

### *Right to withdrawal*

The right to withdrawal, foreseen by the Directive 97/7 on consumer protection with respect to distance contracts, may not apply (unless otherwise agreed) to contracts in which (a) the provision of services has begun with the consumer's agreement before the end of the seven-working-day period and (b) goods have been made to the consumer's specifications or clearly personalised or which, by their nature, cannot be returned or are liable to deteriorate or expire rapidly.

*In an AmI world, services will be provided instantly and will be increasingly personalised. This implies that the right of withdrawal will become inapplicable in many cases. New solutions should be developed to address this problem.*

---

[313] Tribunal de grande instance de Nanterre, 2 June 2004 (*UFC Que Choisir* v. *AOL Bertelsmann Online France*), available at http://www.legalis.net/jurisprudence-decision.php3?id_article=1211. For an English analysis, see Naylor, David, & Cyril Ritter, "B2C in Europe and Avoiding Contractual Liability: Why Businesses with European Operations Should Review their Customer Contracts Now", 15 September 2004. http://www.droit-technologie.org

[314] Currently, insofar as it is not received on a permanent medium, consumers must also receive written notice in good time of the information necessary for proper performance of the contract.

### *Temporary accounts*

In AmI, payments will often occur automatically, at the moment of ordering or even offering the service.

*Temporary accounts, administered by trusted third parties, could temporarily store money paid by a consumer to a product or service provider. This can support consumer protection and enforcement, in particular with respect to fraud and for effectively exercising the right of withdrawal.* This would be welcome for services that are offered to consumers in the EU by service providers located in third countries, as enforcement of consumer protection rights is likely to be less effective in such situations.

### *Group litigation and consumer claims*

The possibility of group consumer litigation[315] can increase the level of law enforcement and, especially, enforcement of consumer protection law. Often an individual claim does not represent an important economic value, thus, individuals are discouraged from making efforts to enforce their rights.

*Launching collective claims or similar actions would increase the effective power against service providers. A similar solution is now available at European level in the case of injunctions*.

Bodies or organisations with a legitimate interest in ensuring that the collective interests of consumers are protected *can* institute proceedings before courts or competent administrative authorities and seek termination of any behaviour adversely affecting consumer protection and which is defined by law as illegal.[316] However, as far as actions for damages are concerned, issues such as the form and availability of the group litigationare regulated by the national laws of the Member States as part of procedural law. The possibility to bring such a claim is restricted to a small number of states.[317]

---

[315] Group litigation is a broad term which captures collective claims (single claims brought on behalf of a group of identified or identifiable individuals), representative actions (single claims brought on behalf of a group of identified individuals by, e.g., a consumer interest association), class action (one party or group of parties may sue as representatives of a larger class of unidentified individuals), among others. These definitions as well as the procedural shape of such claims vary in different Member States. Waelbroeck D., D. Slater and G. Even-Shoshan G [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, pp. 44. http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.html. The SWAMI consortium abstains from designating one of those forms as adequate. Instead, we recommend to the adequate authority to further study the issue, however, which points to the controversial character of class actions on European grounds and thus proposes to focus on other possible forms.

[316] Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 On injunctions for the protection of consumers' interests, *Official Journal* L 166, 11/06/1998, pp. 51 – 55.

[317] Belgian law provides that in certain circumstances associations can bring collective damage action or action for several individual damages. Waelbroeck D., D. Slater and G. Even-Shoshan [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, pp. 44-47.
http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.html

### 10.3.7 Specific recommendations regarding electronic commerce

#### *The scope of the e-commerce directive*

The e-commerce directive[318] aims to provide a common framework for information society services in the Member States of the EU (see the first SWAMI report). An important feature of the directive is that it also applies to legal persons. Similar to the consumer protection legislation, the directive foresees an obligation to provide certain information to customers. In view of the increasing number of service providers, it may not be feasible to provide information about all of them. *Providing information about the service provider whom the customer pays directly and who is responsible towards him could be a solution to the problem of the proliferating number of service providers (joint liability may also apply here). The directive should also be updated to include the possibility of concluding contracts by electronic means (including reference to intelligent agents) and to facilitate the usage of pseudonyms, trusted third parties and credentials in electronic commerce.*

#### *Unsolicited communication (spam)*

Unsolicited commercial communication is an undesirable phenomenon in cyberspace. It constitutes a large portion of traffic on the Internet, using its resources (bandwidth, storage capacity) and forcing Internet providers and users to adopt organisational measures to fight it (by filtering and blocking spam). Spam can also constitute a security threat.[319] The SWAMI dark scenarios show that spam may become an even more serious problem than it is today. [320] An increase in the volume of spam can be expected because of the emergence of new means of electronic communication. Zero-cost models for e-mail services encourage these practices, and similar problems may be expected when mobile services pick up a zero-cost or flat-fee model.

As we become increasingly dependent on electronic communication – ambient intelligence presupposes that we are almost constantly on-line – we become more vulnerable to spam. In the example from the first SWAMI dark scenario, spamming may cause irritation and make the individual reluctant to use ambient intelligence. Fighting spam may well demand even more resources than it does today as new methods of spamming – such as highly personalised and location-based advertising – emerge.

Currently, many legal acts throughout the world penalise unsolicited communication, but without much success. The Privacy and Electronic Communication Directive 2002[321] provides for an opt-in regime, applicable in the instance of commercial communication,

---

[318] 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, pp. 0001 – 0016.

[319] Sorkin, David E., "Technical and Legal Approaches to Unsolicited Electronic Mail", *University of San Francisco Law Review*, Vol. 35, 2001, p. 336 and following.

[320] Punie, Y., S. Delaitre, I. Maghiros & D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities,* SWAMI Deliverable D 2, November 2005, Scenario 1 situation 2, p. 18 and p. 91

[321] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) *Official Journal* L 201, 31/07/2002, pp. 37- 47.

thus inherently prohibiting unsolicited marketing.[322] Electronic communications are, however, defined as "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."[323] The communications need to have a commercial content in order to fall under the opt-in regulation of Directive 2002/58/EC.[324]

Consequently, this directive may not cover unsolicited, location-based advertisements with a commercial content that are broadcast to a group of people ("the public"). The impact of this exception cannot be addressed yet since location-based services are still in infancy.

*A broad interpretation of electronic communications is necessary (the directive is technology-neutral). Considering any unsolicited electronic communication as spam, regardless of the content and regardless of the technological means, would offer protection that is adequate in ambient intelligence environments in which digital communications between people (and service providers) will exceed physical conversations and communications.*[325]

### 10.3.8 Specific recommendation regarding liability law

#### *General*

Civil damages address a harm already done, and compensate for damages sustained. Effective civil liability rules might actually form one of the biggest incentives for all actors involved to adhere to the obligations envisaged by law. One could establish liability for breach of contract, or on the basis of the general tort rules. To succeed in court, one has to prove the damage, the causal link and the fault. Liability can be established for any damages sustained, as far as the conditions of liability are proven and so long as liability is not excluded (as in the case of some situations in which intermediary service providers are involved[326]). However, in AmI, to establish such proof can be extremely difficult.

---

[322] Andrews, S., *Privacy and human rights 2002*, produced by the Electronic Privacy Information Center (EPIC), Washington D.C. and *Privacy International*, London, 2002, p.12. http://www.privacyinternational.org/survey/phr2002/

[323] Article 2 (d) of Directive 2002/58/EC.

[324] Recital 40 states, "Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient."

[325] Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", *op.cit*; Schreurs, W., "Spam en electronische reclame [Spam and electronic communication]", *Nieuw Juridisch Weekblad,* 2003-48, pp. 1174 - 1185.

[326] Articles 12 to 15 of the 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, pp. 1-16. The Directive provides for exceptions to the liability for Intermediary Service Providers (ISPs) under certain conditions. In the case of hosting, for example, a service provider is not liable for the information stored at the request of a recipient of the service, on condition that (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from

As we have seen in SWAMI's dark scenarios, each action is very complex, with a multiplicity of actors involved, and intelligent agents acting for service providers often undertake the action or decision causing the damage. Who is then to blame? How easy will it be to establish causation in a case where the system itself generates the information and undertake the actions? How will the individual deal with such problems? The individual who is able to obtain damages addressing his harm in an efficient and quick way will have the incentive to actually take an action against the infringer, thus raising the level of overall enforcement of the law. Such an effect would be very desirable, especially since no state nor any enforcement agency is actually capable of providing a sufficient level of control and/or enforcement of the legal rules.

The liability provisions of the e-commerce directive can become problematic. The scope of the liability exceptions under the directive is not clear. The directive requires ISPs to take down the content if they obtain knowledge on the infringing character of the content (notice and take down procedure). However, the lack of a so-called "put back" procedure (allowing content providers whose content has been wrongfully alleged as illegal, to re-publish it on the Internet) or the verification of take-down notices by third parties is said to possibly infringe freedom of speech.[327]

*It is recommended that the liability rules be strengthened and that consideration be given to means that can facilitate their effectiveness.*

### *Liability for infringement of the privacy law*

We need to further examine the specific rules on liability for infringement of privacy and data protection law, including security infringements. Currently, the right to remedy in such circumstances is based on the general liability (tort) rules. The data protection directive refers explicitly to liability issues stating that an immediate compensation mechanism shall be developed in case of liability for an automated decision based on inadequate profiles and refusal of access .However, it is not clear whether it could be understood as a departure from general rules and a strengthening of the liability regime. Determining the scope of liability for privacy breach and security infringements might also be problematic. In any case, the proof of the elements of claim and meeting the general tort law preconditions (damage, causality and fault) can be very difficult.

*Opacity instruments, as discussed above, aiming to prohibit the interference into one's privacy can help to provide some clarity as to the scope of the liability. In addition, guidelines and interpretations on liability would be generally welcome, as well as standards for safety measures, to provide for greater clarity and thus greater legal certainty for both users and undertakings.*

---

which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

[327] See Sutter Gavin, "'Don't Shoot the Messenger?' The UK and Online Intermediary Liability", *International Review of Law Computers & Technology*, Vol. 17 No.1, 2003, pp. 73-84; Julia-Barcelo, R., and K. J. Koelman, "Intermediary Liability in the E- commerce Directive: So far so Good, But It's not Enough", *Computer Law and Security Report*, Vol. 16, No. 4, 2000, pp. 231-239.

### *Joint and several liability*

As already mentioned, it can be troublesome for a user to point at the party who is actually responsible for the damages caused, especially if he or she does not know which parties were actually involved in the service and/or software creation and delivery.

*The user should be able to request compensation from the service provider with whom he or she had direct contact in the process of the service. Joint and several liability (with the right to redress) should be the default rule in the case of the providers of AmI services, software, hardware or other products, both in contractual and extra contractual liability cases. Complexity of the actions and multiplicity of actors justifies such a position.*[328] Moreover, this recommendation should be supplemented by the consumer protection recommendation requiring the provision of consumer information by the service or product provider having the closest connection with the consumer, as well as the provision of information about the individual privacy rights (see above) in a way that would enable the individual to detect a privacy infringement and have a better chance to prove it in court. There is a need to consider the liability regime with other provisions of law.

### *Strict liability*

The product liability directive[329] provides for a liability without fault (strict liability).[330] As the recital to the Directive states, strict liability shall be seen as "the sole means of adequately solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production." We should keep this reasoning in mind since it seems even more adequate when thinking about the liability issues in AmI.

Most of the "products" offered in the AmI environment will consist of software-based, highly personalised services. We should then think about adjusting the liability rules to such an environment. If it is difficult to distinguish between hardware and software from a technological perspective, why should we draw such a distinction from a legal perspective?[331] *An explicit provision providing for strict liability for software can be considered.*[332] Nevertheless, such a proposal is regarded as controversial. It is said to threaten industry. Since software is never defect-free, strict liability would expose software producers unfairly to the damages claims. Thus, the degree of required safety of the programs is a policy decision.[333] Strict liability could also impede innovation, especially

[328] Joint and several liability is already foreseen in the product liability directive.
[329] 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, pp.29 –33.
[330] A strict product liability regime based on the directive is the basis of the claims under the general tort regime. See Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", *Netherlands Comparative Law Association*, 2002, pp. 75-79. http://www.ejcl.org/64/art64-6.html.
[331] Hilty, Lorenz, 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, p. 269.
[332] In such a case, the intelligent software agent's failure and the PET's failure might be covered by the strict liability regime. Special derogation for PETs could be envisaged.
[333] 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, 2001, p. 204.

the innovation of new, experimental and life-saving applications.[334] Others argue that strict liability might increase software quality by making producers more diligent, especially, in properly testing the product.[335]

Despite these policy considerations, there are some legal questions about the applicability of strict liability to software. The first issue to answer is whether the software can be regarded as "goods" or "products" and whether they fall under the strict liability regime.[336] In fact, the answer to that question depends on the national laws relating to those issues and implementing the directive. The directive applies to products defined as all movables[337], which might suggest that it refers to goods having a tangible medium. Software not incorporated into the tangible medium (available on-line) will not satisfy such a definition. There are a growing number of devices (products) with embedded software (e.g., washing machines, microwaves, possibly RFIDs), which fall under the regime of the directive today.[338] Such a tendency will continue, though the software application will be increasingly crucial for the proper functioning of the products themselves, services and whole environments (smart car, smart home). Should the distinction between the two regimes remain?

Strict liability is limited to death or personal injury, or damage to property intended for private use.[339] The damage relating to the product itself, to the product used in the course of business and the economic loss, will not be remedied under the directive.[340] Currently, defective software is most likely to cause financial loss only, thus the injured party would not be able to rely on provisions of the directive in seeking redress. However, even now in some life-saving applications, personal injury dangers can emerge. Such will also be the case in the AmI world (see, for example, the first and second SWAMI dark scenarios in which software failures cause accidents, property damage and personal injury) so the importance and applicability of the product liability directive will grow. The increasing dependence on software applications in everyday life, the increasing danger of sustaining personal injury due to a software failure and, thus, the growing concerns of consumers justify strengthening the software liability regime.

However, the directive allows for a state-of-the-art defence. Under this defence, a producer is not liable if the state of scientific and technical knowledge at the time the product was put into circulation was not such that the existence of the defect would be discovered. It has been argued that the availability of such a defence (Member States have the discretion

---

[334] Singsangob A., *Computer Software and Information Licensing in Emerging Markets, The Need for a Viable Legal Framework*, Aspen Publishers, 2003, p. 113.

[335] Desai, M.S., J. Oghen and T.C. Richards, "Information Technology Litigation and Software Failure", *The Journal of Information, Law & Technology*, 2002 (2). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/desai/. Compare with coments on softwere testing under 2.3. and 4.2.6.

[336] Similar discussion takes place in the US. It seems that, despite the fact that the issue is not clearly stated, there is a tendency to regard software as a good, especially if the parties to the contract intended to treat it as such (as opposed to an information service). See Singsangob A., *Computer Software and Information Licensing in Emerging Markets, The Need for a Viable Legal Framework*, Aspen Publishers , 2003, p. 113.

[337] Article 2 of the Directive.

[338] Reed, Ch., and A. Welterveden, "Liability", in Ch. Reed and J. Angel (eds.), *ComputerLaw*, London 2000, p. 99.

[339] Article 9 of the Product Liability Directive.

[340] Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", *Netherlands Comparative Law Association*, 2002, p. 82, http://www.ejcl.org/64/art64-6.html

whether to retain it in the national laws or not[341]) will always be possible since, due to the complexity of "code", software will never be defect free.[342]

The above-mentioned policy arguments as well as the legal arguments show the difficulty in broadening the scope of the strict liability directive to include software, but they might also point to an alternative solution. Reversal of the burden of proof might be a more adequate solution. Policy-makers should investigate which solution is best.

As mentioned, it is often difficult to distinguish software from hardware: both are necessary and interdependent to provide a certain functionality. Similarly, it may be difficult to draw the line between software and services. Transfer of information via electronic signals (e.g., downloaded software) could be regarded as a service.[343] Some courts might also be willing to distinguish between mass-market software and software produced as an individual product (on demand). AmI is a highly personalised environment where the software-based services will surround the individual, thus the tendency to regard software as a service could increase.

Strict liability currently does not apply to services. Service liability is regulated by national laws.[344] Extending such provision to services can have far-reaching consequences, not only in the ICT field. The AmI environment will need the innovation and creativity of service providers; therefore one should refrain from creating a framework discouraging them from taking risks. However, some procedural rules could help consumers, but without upsetting an equitable balance. The consumer, usually the weaker party in a conflict with the provider, often has difficulty proving damages. Reversing the burden of proof might facilitate such proof. Most national laws seem to provide a similar solution.[345]

*Since national law regulates the issue of service liability, differences between national regulations might lead to differences in the level of protection. The lack of a coherent legal framework for service liability in Europe is regrettable. Learning from the differences and similarities between the different national legal regimes, as indicated in the Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services,[346] is the first step in remedying such a situation.*

### *Reversing the burden of proof*

Reversing the burden of proof is less invasive than the strict liability rules, when the issue of fault is simply not taken into consideration. Such a solution has been adopted in the field of the antidiscrimination and intellectual property laws, as well as in national tort

[341] Article 15(1)(b) of the Product Liability Directive.
[342] 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, 2001, p. 204.
[343] The OECD has treated software downloads as a service for the VAT and custom duties purposes; see Henderson, K., and A. Poulter, "The Distance Selling Directive: Points for Further Revision", *International Review for Law Computers & Technology*, Vol. 16 no. 3, 2002, p. 289-300.
[344] As a basis for liability, the contractual liability or the fault-based tort liability applies. See Giensen, I., and M.B.M. Loos, *l.c.*as well as Magnus, U., and H.W. Micklitz, *Comparative Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services*: A study commissioned by the European Commission, Final Report, Part D: The Comparative Part, April 2004, p. 62.
http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf
[345] Magnus, U., and H.W. Micklitz, p. 8.
[346] Magnus, U., and H.W. Micklitz, p. 8.

systems.[347] An exception to the general liability regime is also provided in Directive 1999/93/EC on the community framework for electronic signatures.[348] The certification service provider is liable for damage caused by non-compliance with obligations imposed by the directive[349], unless he proves he did not act negligently.[350] It is an example of reversal of burden of proof, the solution the SWAMI consortium proposes be considered for ICT service liability.

Technology could potentially remedy the information asymmetry between users and AmI service suppliers or data processors. The latter could have an obligation to inform consumers what data are processed, how and when and what is the aim of such activities (thus actually fulfilling their obligations under the data protection directive). This information could be stored and managed by an intelligent agent on behalf of the user, who is not able to deal with such information flow. However, the user would have the possibility to use such information to enforce his rights (e.g., to prove causation). Other technological solutions (e.g., watermarking) could also help the user prove his case in court.

### *Consumer claims and fixed damages*

In many cases, the damage sustained by the individual will be difficult to assess in terms of the economic value or too small to actually provide an incentive to bring an action to court. However, acts causing such damage can have overall negative effects. Spam could be a good example. *Fixed damages, similar to the ones used in the US, or punitive damages could remedy such problems (some US state laws provide for fixed damages such as US$200 for each unsolicited communication without the victim needing to prove such damage). They would also provide clarity as to the sanctions or damages expected and could possibly have a deterrent effect.* The national laws of each Member State currently regulate availability of punitive damages; a few countries provide for punitive and exemplary damages in their tort systems.[351]

Actions allowing consolidation of the small claims of individuals could be also examined (i.e., group consumer actions).

---

[347] Magnus, U., and H.W. Micklitz, *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.
http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportabc_en.pdf
http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf

[348] On issues relating to digital signatures, see Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005. http://www.fidis.net. See also 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 013, 19/01/2000, pp. 0012-002. For commentary on the directive, see Friedewald, M., E. Vildjiounatie and D. Wright (eds.), *The brave new world of ambient intelligence: A state-of-the-art review*, SWAMI Deliverable D 1, July 2005, p. 167.

[349] For example, the service provider is liable for the inaccuracy or incompleteness of the information contained in the certificate at the tame the certificate was issued.

[350] The liability rules described above seem sufficient as a legal framework for qualified digital signatures. The general tort rules apply in relation to liability in all other cases (other than qualified signatures).

[351] There are also not enough sources to state if they would apply in anti-spam cases. Available sources refers here to antitrust claims. Waelbroeck D., D. Slater and G. Even-Shoshan [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, pp. 44-47.
http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.htm

### 10.3.9 Specific recommendation regarding equality law

#### *What is non- discrimination law?*

Non-discrimination law can regulate and forbid the unlawful usage of data processed, e.g., in making decisions or undertaking other actions on the basis of certain characteristics of the data subjects. This makes the non-discrimination law of increasing importance for AmI. The *creation* itself of profiles does not fall under the non-discrimination law[352] (potential use), but decisions based on profiling (including group profiling based on anonymous data) which affects the individual might provide the grounds for application of the non-discrimination rules. They apply in case of the identifiable individuals but also to anonymous members of the group.[353]

Profiles or decisions based on certain criteria (health data, nationality, income, etc.) may lead to discrimination against individuals. It is difficult to determine when it is objectively justified to use such data and criteria, and when they are discriminatory (for instance, the processing of health-related data by insurance companies leading to decisions to raise premiums). Further legislative clarity would be desirable.

However, certain negative dimensions of profiling still escape from the regime of non-discrimination law (e.g., manipulation of individuals' behaviour by targeted advertising). Here no remedies have been identified.

The non-discrimination rules should be read in conjunction with the fairness principle of data protection law. The application of the two may have similar aims and effects; they might also be complementary (Can the limitations of non-discrimination law be justified if they are regarded as not fair, as in the example of the insurance companies raising premiums after processing health data?). They can address a range of actions undertaken in AmI, such as dynamic pricing or refusal to provide services (e.g., a refusal of service on the ground that no information (profile) is available could be regarded as discriminatory.).

*Non-discrimination rules should be taken into consideration at the design stage of technology and service development.*

#### *Universal services*

The universal service directive[354] provides for a minimum of telecommunication services for all at an affordable price as determined by each Member State. Prices for universal services may depart from those resulting from market conditions.[355] Such provisions aim at

---

[352] However, such issues might be addressed by the data protection legislation. In the opinion of Gutwirth & De Hert, principles of data protection are appropriate to cope with profiling. Hildebrandt, M. & S. Gutwirth (eds.), *Implications of profiling practices on democracy and rule of law*, FIDIS Deliverable D7.4, September 2005. http://www.fidis.net/fidis_del.html.

[353] Custers, B., *The Power of Knowledge, Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen, 2004, pp. 164-165.

[354] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) *OJ L* 108 , 24/04/2002 p. 0051 – 0077.

[355] More on the directive in Friedewald M., E. Vildjiounatie and D. Wright (eds.), *The brave new world of ambient intelligence: A state-of-the-art review,* SWAMI Deliverable D 1, July 2005, p. 176.

overcoming a digital divide and allowing all to enjoy a certain minimum of electronic services. The directive is definitely a good start in shaping the Information Society and the AmI environment. The development of new technologies and services generate costs, both on individual and the society at large. Many high-added-value AmI services will be designed for people who will be able to pay for them. Thus, AmI will reinforce the inequalities between the poor and rich. However, it has to be ensured that all are enabled to participate in the benefits of AmI, at least at a minimum level. *The Commission should consider whether new emerging AmI services should be provided to all. Some services (e.g., emergency services) could even be regarded as public and provided free of charge or as part of social security schemes.*

### 10.3.10 Specific recommendations regarding interoperability and IPR

#### *General*

The SWAMI deliverables 1 and 2 emphasised that AmI will cause major problems for current intellectual property protection, because AmI requires interoperability of devices, software, data and information, e.g., for crucial information systems such as health monitoring systems used by travelling seniors. There is also the growing need for creating means of intellectual property protection that will respect privacy and allow for anonymous content viewing. Intellectual property rights give exclusive rights over the databases consisting of personal data and profiles, while the data subjects do not have a property right over their own information collected. We discuss these issues below.

#### *Protection of databases and profiling*

The directive on the legal protection of databases[356] provides for a copyright protection of databases, if they constitute the author's own intellectual creation by virtue of his selection or arrangement of their content. The directive also foresees a *sui generis* protection, if there has been a qualitatively and/or quantitatively substantial investment in either the obtaining, verification or presentation of the content. *Sui generis* protection "prevents the extraction and/or the re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database". This implies that the database maker can obtain a *sui generis* protection of a database even when its content consists of personal data. Although the user does not have a property right over his personal data, the maker of a database can obtain an exclusive right over this type of data. Hence, a profile built on the personal data of a data subject might constitute somebody else's intellectual property.

*The right to information about what knowledge has been derived from one's data could, to some extent, provide a safeguard against profiling. We recommend that further research be undertaken on how to reconcile this with the intellectual property rights.*[357]

#### *DRMs*

The copyright directive[358] provides for the protection of DRMs used to manage the licence rights of works that are accessed after identification or authentication of a user.[359] But

[356] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal* L 077, 27/03/1996, pp. 0020 – 0028.
[357] See above, right to information.

DRMs can violate privacy, because they can be used for processing of personal data and constructing (group) profiles, which might conflict with data protection law.

*Less invasive ways of reconciling intellectual property rights with privacy should be considered.*

This not only relates to technologies but also to an estimation of the factual economic position of the customer. For example, the general terms and conditions for subscribing to an interactive television service – often a service offered by just a few players – should not impose on customers a condition that personal data relating to their viewing behaviour can be processed and used for direct marketing or for transfer to "affiliated" third parties.

As the Article 29 Working Party advises, greater attention should be devoted to the use of PETs within DRM systems.[360] In particular, it advises that tools be used to preserve the anonymity of users and it recommends the limited use of unique identifiers. Use of unique identifiers allows profiling and tagging of a document linked to an individual, enabling tracking for copyright abuses. Such tagging should not be used, unless necessary for performance of the service or unless with the informed consent of individual. All relevant information required under data protection legislation should be provided to users, including categories of collected information, the purpose of collecting and information about the rights of the data subject.[361]

The directive on the legal protection of software[362] obliges Member States to provide appropriate remedies against a person committing any act of putting into circulation, or the possession for commercial purposes of any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program. *The software directive only protects against the putting into circulation of such devices and not against the act of circumventing as such. It would be advisable to have a uniform solution in that respect. DRM can also violate consumer rights, by preventing the lawful enjoyment of the purchased product. The anti-circumvention provisions should be then coupled with better enforcement of consumer protection provisions regarding information disclosure to the consumer.* [363] *The consumer should always be aware of any technological measures used to protect the content he wishes to purchase, and restrictions in use of such content as a consequence of technological protection (as well as he should be informed about technological consequences of DRMs for his devices, if any, e.g., installing the software on*

---

[358] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal* L 167, 22/06/2001, pp. 0010 – 0019.

[359] See also above, Privacy Enhancing Technologies.

[360] Article 29 Data Protection Working Party, *Working document on data protection issues related to intellectual property rights* (WP 104), adopted on 18 January 2005.
http://ec.europa.eu/justice_home/fsj/privacy/

[361] Idem.

[362] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17/05/1991, pp. 0042-0046.

[363] See also OECD, *Report on Disclosure Issues Related to the Use of Copy Control and Digital Rights Management Technologies*, DSTI/CP(2005)15/FINAL, 2006.
https://www.oecd.org/dataoecd/47/31/36546422.pdf. For comments on consumer needs re DRM, see also INDICARE Project, "Content Providers' Guide to Digital Rights Management: Any side effects in using DRM?". www.indicare.org.

*the computer of the client).*[364] *Product warnings and consumer notifications should always be in place, as well as raising general consumer awareness on the DRMs.*

#### *Decompilation right*

*As interoperability is a precondition for AmI, AmI would have to lead to limitations on exclusive intellectual property rights. One could actually argue that software should be developed so that they are interoperable with each other. That implies creating standards applicable in this field. Facilitating creation of ICT global standards is desirable for interoperability and privacy protection. Broader scope of the decompilation right under software protection would be desirable.*

The EU's current battle with Microsoft shows that it is trying to strengthen the decompilation right with support of competition law reasoning. Time will show what the outcome of the battle will be.

### 10.3.11 Specific recommendations regarding international co-operation

#### *Jurisdiction in criminal matters*

Currently there is no international or European framework determining jurisdiction in the criminal matters, thus, national rules are applicable. The main characteristics of the legal provisions in this matter have already been extensively discussed in previous SWAMI deliverables; however, it seems useful to refer here to some of our earlier conclusions. The analysis of the connecting factors for forum selection (where a case is to be heard) shows that it is almost always possible for a judge to declare himself competent to hear a case. Certain guidelines have already been developed, both in the context of the Cybercrime Convention[365] as well as the 2005 EU Framework Decision on attacks against information systems[366] on how to resolve the issue of concurrent competences. According to the Cybercrime Convention, "The Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[367]

The 2005 EU Framework Decision on attacks against information systems states, "Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralizing proceedings in a single Member State."[368]

*Legal experts and academics should follow any future developments in application of those rules that might indicate whether more straightforward rules are needed. The discussion*

---

[364] Those restrictions might, *inter alia*, prevent the user from making backups or private copies, downloading music to portable devices, playing music on certain devices, or constitute the geographical restrictions such as regional coding of DVDs.
[365] Council of Europe - Cybercrime Convention of 23 November 2001.
[366] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ* L 069, 16/03/2005 p. 67- 71.
[367] Article 22 paragraph 5 Cybercrime Convention.
[368] Article 10 paragraph 5 *2005 EU Framework Decision on attacks against information systems* raises the possibility of invoking any institutional mechanism to facilitate such co-operation, and factors that should be taken into account when considering an appropriate forum.

*on the recently published Green Paper on double jeopardy should also be closely followed.*[369]

### *Private international law*

In the SWAMI scenario *Journey of the seniors*, we discussed an accident involving German tourists in Italy, while travelling with a tourist company established in a third country. The international dimension of the actions taken in AmI could actually lead to the conclusion that fitting AmI into a legal framework based on territorial concepts might cause some problems. Clear rules determining the law applicable between the parties are an important guarantee of legal certainty.

Private international law issues are dealt at the European level by two legal acts, the Rome Convention on the law applicable to contractual obligations[370] and the Brussels Regulation on jurisdiction and enforcement of judgments[371].

### *Jurisdiction in civil matters*

The Regulation on jurisdiction and enforcement of judgments in civil and commercial matters covers both contractual and non-contractual matters. It also contains provosions for jurisdiction for consumer contracts. This provision should be satisfactory and workable in an AmI environment.

*In cases where the defendant is domiciled outside the EU, the regulation will not provide a solution for forum selection*[372]*, nor do the provisions on the jurisdiction in consumer contracts. This emphasises again the limitation of the discussed solution to the territory of the Member States and the need for a more global approach.*[373]

*Clarification and simplification of the forum selection for non-consumers would also be desirable. It seems that the complexity of the business environment, service/product creation and delivery would justify such approach. It would be of special importance for SMEs.*

---

[369] Green Paper on Conflicts of Jurisdiction and the Principle of *ne bis in idem* in Criminal Proceedings COM(2005) 696, December 2005, accesible at http://ec.europa.eu/comm/off/green/index_en.htm

[370] 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.

[371] 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.

[372] Article 4 of the Brussels Regulation states: 1. If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Articles 22 and 23, be determined by the law of that Member State; 2. As against such a defendant, any person domiciled in a Member State may, whatever his nationality, avail himself in that State of the rules of jurisdiction there in force, and in particular those specified in Annex I, in the same way as the nationals of that State.

[373] Ofcom, the UK regulator for communications, has made a similar point: "the global reach and open nature of the internet gives rise to some well-known problems, which cannot be addressed by a translation of existing powers and structures." *Online protection: A survey of consumer, industry and regulatory mechanisms and systems*, 21 June 2006, p. 1.
http://www.ofcom.org.uk/research/technology/onlineprotection/report.pdf

### *Applicable law*

Currently, the applicable law for contractual obligations is determined by the 1980 Rome Convention.[374] Efforts have been undertaken to modernise the Rome Convention and replace it with a Community Instrument. Recently, the Commission has presented the proposal for a regulation of the European Parliament and the Council on the law applicable to contractual obligations.[375]

The biggest weakness of the Rome Convention seems to be its limitation to contractual issues only. Although contracts will be crucial for the AmI environment, it is more than desirable to provide a clear set of rules for non-contractual relationships. Some initiatives have already been undertaken in that direction.[376]

A feature of the Rome Convention is that it relies heavily on the territorial criterion. It refers to the habitual residence, the central administration or place of business as the key factors determining the national law most relevant to the case.[377] But IT services can be supplied at a distance by electronic means. The AmI service supplier could have his habitual residence or central administration anywhere in the world and he could choose his place of residence (central administration) according to how beneficial is the national law of a given country. The habitual residence factor has been kept and strengthened in the Commission's proposal for a new regulation replacing the Rome Convention (Rome I proposal, Article 4).[378]

The new proposal for the Rome I regulation amends the consumer protection provisions.[379] It still relies on the *habitual residence* of the consumer, but it brings the consumer contract choice of law in line with the equivalent provisions of the Brussels regulation, and broadens the scope of the application of its provisions. The Commission proposal for the regulation on the law applicable to contractual obligations is in any event a good step forward.

---

[374] 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 pp. 0001-0019.

[375] The Commission has presented the proposal for a regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I), COM (2005) 650 final, 2005/0261 (COD).

[376] We refer here to the Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations ("Rome II"), COM(2003) 427 final 2003/0168 (COD). http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0427en01.pdf

[377] According to Article 4, "the contract shall be governed by the law of the country with which it is most closely connected." Article 4 further reads: "It shall be presumed that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporated, its central administration. However, if the contract is entered into in the course of that party's trade or profession, that country shall be the country in which the principal place of business is situated or, where under the terms of the contract the performance is to be effected through a place of business other than the principal place of business, the country in which that other place of business is situated."

[378] The new proposal does not use the presumption that the country of habitual residence is the most closely connected with the case, as it is under the Rome Convention. In the proposal, the relevant factor of the habitual residence of, *inter alia*, seller or service provider is the fixed rule.

[379] As recital 10 of the proposal states, these amendments aim to take into account the developments in distance selling, thus including ICT developments.

Some other legislative acts also contain rules on applicable law. Most important are provisions in the data protection directive. This directive also chooses the territorial criterion to determine the national law applicable to the processing of data, which is the law of the place where the processing is carried out in the context of the activities of an establishment of the data controller. Such a criterion, however, might be problematic: more than one national law might be applicable to the case.[380] Moreover, in times of globalisation of economic activity, it is easy for an undertaking to choose the place of establishment, which would guarantee him the most liberal regime, which might avoid the application of the European data protection law. In situations when a non-EU state is involved, the directive points out to a different relevant factor, the location of the equipment used[381], thus enabling broader application of the EU data protection directive.[382]

As we see, in all these cases, the territorial criterion (establishment) prevails. *We should consider moving towards a more personal criterion, especially since personal data are linked with an identity and a state of a data subject (issues which are regulated by the national law of the person). Such a criterion could be more easily reconciled with the AmI world without the physical borders of high mobility.* The data subject will also be able to remain under the protection of his/her national law, and the data controller/service provider will not have the possibility of selecting a place of establishment granting him the most liberal treatment of law.[383]

### *Data transfer*

Data transfer is another issue emphasising the need for international co-operation in the creation of a common playing field for AmI at the global level. What is the sense of protecting data in one country if they are transferred to a country not affording comparable (or any) safeguards? Also, the globalisation of economic and other activities brings the necessity of exchanging personal data between the countries. The data protection directive

---

[380] Article 4 (1) of the directive stipulates: Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

[381] The directive stipulates in article 4 (1) that the national law of a given Member State will apply when the controller is not established on Community territory and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

[382] The Article 29 Data Protection Working Party interprets the term "equipment" as referring to all kinds of tools or devices, including personal computers, which can be used for many kinds of processing operations. The definition could be extended to all devices with a capacity to collect data, including sensors, implants and maybe RFIDs. (Active RFID chips can also *collect* information. They are expensive compared to passive RFID chips but are already part of the real world.) See Article 29 Data Protection Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites* (5035/01/EN/Final WP 56), 30 May 2002. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

[383] Such a solution has the advantage of covering, with the protection of EU legislation, third country residents whose data are processed via equipment in the EU. A broad interpretation of the term "equipment" would help guarantee the relatively broad application of such rule (see above). As a result, in most cases, application of the domicile/nationality rule or the place of the equipment used as the relevant factor would have the same result. However, we can envisage the processing of data not using such equipment, for example, when the data are already posted on-line. Then the EU law could not be applicable.

provides a set of rules on the data transfer to the third countries.[384] The data can be transferred only to countries offering an adequate level of protection. The Commission can conclude agreements (e.g., the Safe Harbour Agreement) with third countries that ensure an adequate level of protection. The Commission can also issue a decision in that respect. However, the major problem is again enforcement of such rules, especially in view of the fact that some "safeguards" rely on self-regulatory systems whereby companies merely promise not to violate their declared privacy policies (as is the case with the Safe Harbour Agreement*). Attention by the media and consumer organisations can help in the enforcement of agreed rules. The problem of weak enforcement also emphasises the need to strengthen international co-operation with the aim of developing new enforcement mechanisms. Providing assistance in good practices in countries with less experience than the EU might also be very useful.*

[384] On 30 May 2006, the European court of justice ruled that it was unlawful to order European airlines to hand over information about transatlantic air passengers to the US government. The court said the US did not provide adequate protection for air passengers' privacy. Under the Passenger Name Records agreement, reached in May 2004, EU airlines have been obliged to give Washington 34 items of information about passengers flying to the US. The court said the agreement had to be annulled because existing EU data protection law only covers commercial data and not that used for security purposes. See Sturcke, James and agencies, "US access to flight data unlawful", *The Guardian*, 30 May 2006.

# 11 CONCLUSIONS AND RECOMMENDATIONS FOR STAKEHOLDERS

In the previous chapter, the partners identified safeguards against the threats and vulnerabilities affecting privacy, identity, trust, security and the digital divide in an AmI world. We commend implementation of these safeguards. In this chapter, we offer some specific recommendations addressed to particular stakeholders some of which flow from the safeguards identified above.

## 11.1 ADOPTING A RISK ASSESSMENT – RISK MANAGEMENT APPROACH TO AMI

Since their creation, the Internet and the World Wide Web have become a critical infrastructure, arguably *the* critical infrastructure in virtually all countries and all societies. The Internet's interconnectedness and the dependency of other critical infrastructures (banking, transport, telecoms, electricity, water, etc.) upon it have made it indispensable to the functioning of our societies and economies. Further, many people now use the Internet more every day than they watch TV. As exponential as has been its growth and as pervasive as it has become, the Internet is just a stepping stone on the way to an even more pervasive network and set of technologies that will provide us with ambient intelligence.

Yet the development and implementation of ambient intelligence is taking place with little involvement of the wide range of stakeholders in an assessment of the risks (especially to security) that it poses. And, it's important to recall, risks are not static. Risks are growing as things become more interconnected.[385] No one has yet called for the rigour of a formalised risk assessment / risk management process for deployment of AmI even though it will have far-ranging impacts on our way of life. AmI offers great benefits, but poses great risks too.

Of course, no such process was followed when the Internet was constructed, but that is no reason to forsake such a process for AmI. Also, most people in the early 1990s were unaware of the coming of the Internet and the WWW, nor of how quickly they would take root. Such is not the case with AmI. Many people know AmI is coming and many experts have already starting raising yellow flags of caution: despite its many benefits, AmI will not be risk free.

Some people undoubtedly, and perhaps even justifiably, might argue that the development of ambient intelligence per se does not require a formalised risk assessment / risk management process. But, if anything, SWAMI hopes and trusts it has demonstrated from its reports that ambient intelligence, as wonderful as it may seem, is not risk free, that it poses serious risks, not only to our privacy (and, as a consequence, to our democratic values), but also to our security (societal safety).

What is especially new or different about an AmI world compared to today's world (or, even better, compared to the pre-Internet world) is the *scale* of data generated, the

[385] "As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities." OECD *Guidelines for the Security of Information Systems and Networks: Towards a culture of security*, OECD, Paris, 2002, p. 7. The OECD has made the point in other of its reports too. See, for example, *Emerging Risks in the 21st Century*, 2003, p. 13: "The openness and connectedness of systems and … technology and information increase the number of potential interactions that can generate or influence a hazard. Risks become more complex."

omnipresence and pervasiveness of the new technologies and, consequently, the scale of the risks that arise from (theoretically) connecting everything and everybody.

Given the magnitude of risks, not just to privacy, but also to security, it seems eminently reasonable (at least to the SWAMI partners) that a formalised risk assessment / risk management process should be initiated to consider the risks posed by AmI and the optimum way of treating them. Risk can never be eliminated, but some ways of treating risks are better than others. The key is involving stakeholders in the process in order to determine what ways of treating risks are the most socially acceptable, that have the most consensus of stakeholders.

We think all stakeholders should have the opportunity to participate in the process of assessing and managing the risks posed by AmI.

We are not alone in thinking so. In its guidelines towards a culture of security, the OECD has emphasised that "all participants are responsible for the security of information systems and networks" and that "participants should conduct risk assessments". Further, it has been said that "security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats".[386]

We would not expect the outcome of any risk assessment – risk management process to call a halt to the deployment of AmI. Even if that were desirable, it is not practicable, nor feasible. In any event, deployment of AmI technologies has already begun.

We recommend that the Commission should initiate a consultation process. It could proceed by announcing the initiation of such a process and invite comments, as the UK House of Lords is doing on the issue of personal Internet security or it could prepare an initial consultation document on AmI, outlining its benefits, threats and vulnerabilities, identify stakeholder groups and solicit their views with regard to those threats and vulnerabilities and the best ways of managing the risks, i.e., the ways that enjoy the widest support of stakeholders.

We think that a formalised risk assessment – risk management process would, if nothing else, help to raise awareness of AmI and the risks it poses. Consulting concerned citizens and those who represent citizens (including legislators) at the stage of development would increase the legitimacy of new technologies, how they should be deployed and used.

The Commission has invited the private sector to "Involve the insurance sector in developing appropriate risk management tools and methods to tackle ICT-related risks and foster a culture of risk management in organisations and business (in particular in SMEs)"[387]. SWAMI agrees with and supports this encouragement from the Commission, particularly, because "risk management tools and methods" have not much of a history in being applied to high tech social and security risks such as ambient intelligence. A

[386] OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security, OECD, Paris, 2002, pp. 10-12.

[387] European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006], p. 9 (section 3.3.2). http://ec.europa.eu/information_society/doc/com2006251.pdf

Commission staff paper has also suggested that one option to improve the security of communication networks is to implement and maintain adequate risk management systems based on recognized international standards.[388] However, while it is good that the Commission recognises the value of applying risk management tools and methods to ICT-related risks, we do not think that this Commission goes far enough, particularly in involving all stakeholders, as we recommend.[389] Furthermore, the aforementioned option would involve EU legislation imposing detailed technical and organisational obligations for providers of electronic communications networks and/or services, whereas SWAMI recommends that the Commission initiate the risk management process described above. We agree with the Commission when it says, "Identifying and meeting security challenges in relation to information systems and networks in the EU requires the full commitment of all stakeholders" [390], but getting that commitment, there's the rub. In order to get that commitment, stakeholders must be given and encouraged to play a meaningful role from the outset of the risk management process, rather than simply leaving it up to the private sector and the insurance industry to devise some appropriate tools.

## 11.2 Recommendations for the European Commission

### 11.2.1 Research and development

The development of AmI safeguards should be supported as much as possible, especially because they are the main means expected to help protect people from accidental, unintentional privacy violation.

Further harmonisation of standards with varying degrees of geographical scope will be needed (e.g., EU, international). Some countries, however, will not be able to afford to fully comply with the standards created in developed countries. Solutions to overcome the potential divides based on insufficient interoperability need to be envisaged.

The Commission should ensure that privacy, identity, trust, security and digital divide issues are taken into account in any project it supports. As has been demonstrated, it is crucial to integrate privacy and security aspects from the very beginning in any development process. Once certain technical platforms, standards or system designs are established, it is often too late or associated with unreasonably high additional costs to adequately include appropriate safeguards.

Research on technologies that could help protect our privacy and strengthen the security of networks and devices (against attackers and other vulnerabilities), and that could help to

[388] Impact Assessment: Commission Staff Working Document, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the EU Regulatory Framework for electronic communications networks and services, SEC(2006) 817, Brussels, 28 June 2006, p. 27.
http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/public_consult/review/impactassessment_final.pdf.

[389] In this context, it is useful to note the UK House of Lords Select Committee on Science and Technology has initiated an investigation into personal Internet security and has opened its consultation to all, including the public, by inviting comments and inputs by the end of October 2006. It plans to issue a report in the summer of 2007. See Williams, Alun, "House of Lords to investigate Net security", PCPro, 28 July 2006.
http://www.pcpro.co.uk/news/91105/house-of-lords-to-investigate-net-security.html

[390] COM(2006) 251, section 4.

minimise the digital divide should be increased. Certain problems cannot be solved by other than technology means: if there are no human-technology interfaces for all categories of possible users (including disabled users or people capable of speaking only one language), then the digital divide will continue to exist. If no user-friendly security exists, security recommendations will not be followed.

Hence concrete, step-by-step initiatives such as the EC-initiated consultation on RFIDs in March 2006[391] are to be welcomed. Further research on the RFID technology and its privacy implications is recommended. This research should also aim at determining whether any legislative action is needed to address the specific privacy concerns of RFID technology. We also recommend further development of codes of conducts and good practices with regard to the use of RFIDs.

Similar consolations with regard to other relevant technologies and concepts, e.g., biometrics and interoperability, could be considered. The implications for privacy caused by other technologies, such as location-tracking systems, physiological sensors, video and audio sensors should be evaluated, and good practices in use of these technologies should be developed and widely promulgated.

### 11.2.2 Internal market and consumer protection

*Prevent discriminatory service refusal*

Effective safeguards to reduce the possibility of ill-founded service refusals mainly apply to the regulatory sphere.

- Regulations and user-friendly tools (which present all relevant information in concise and impressive form, perhaps with examples of possible negative consequences) need to provide for sufficient transparency. This would contribute to strengthening the customers' position and serve as a limitation to the exploitation of asymmetric power relations.
- AmI applications should be implemented preferably on the basis of an opt-in option (the user explicitly chooses to accept the application). In cases when applications are built in such a way that they are constantly attentive to all people around (e.g., to all visitors of a smart space), an option to opt-out needs to be incorporated, confining disadvantages as far as possible.
- Alternative procedures need to be available at reasonable cost in case of technical failures or if individuals request access without having the ability to meet the technical standards.
- Users should have the option to switch off different functionalities of personal devices independently of each other, unlike the current situation when many types (although not all) of mobile phones keep wireless connection always on when the phone is switched on, so that it is impossible to use, for example, the calendar application without your service provider's being aware of your current location.

By the same token, individuals should have the option to switch off their personal AmI devices (either completely or selected functionalities, e.g., to switch off wireless communication) so that even if they are being captured by surveillance cameras, their own devices are not contributing to their being tracked. Effective, free, informed and specific

[391] http://www.rfidconsultation.eu/

consent should be the basis of the EU policy regarding the internal market and consumer protection.

*Prevent victimisation*

As in the case of service refusals, in order to reduce the adverse side-effects of victimisation based, for instance, on faulty profiling, secondary back-up procedures need to be in place, incorporating additional contextual information which enable authorities to take informed decisions without being entirely dependent upon a technical system.

*Electronic commerce and consumer protection*

The e-commerce directive should be updated to include the possibility of concluding contracts by electronic means (including reference to intelligent agents). In any updating of the directive, there is also a need to facilitate the usage of pseudonyms, trusted third parties and credentials in electronic commerce. Intelligent agents could also assist consumers in the management of (electronic) information to which, under the law, they are entitled.

An increasing number of service providers will be involved in AmI services and it may not be feasible for all of them to provide the required information about their data processing activities to consumers. One solution may be a requirement to provide such information about only the service provider whom the consumer directly pays and who is responsible to the consumer (joint liability would apply).

In an AmI world, services will be provided instantly and will be increasingly personalised. In many cases, the right of the consumer to withdraw from the service may not be applicable, feasible or practicable. New solutions should be developed to address this problem.

### 11.2.3 Privacy and security policy framework

On 31 May 2006, the Commission issued a communication in which it proposed a strategy for a secure Information Society.[392] SWAMI agrees with and supports the measures set out in the communication, however, as mentioned elsewhere in this document, we do not think that it goes far enough. The strategy proposes measures that the Commission itself, Member States, the private sector and individuals can take to combat the bad guys who are responsible for attacking our network and information security. There is an implicit assumption that the bad guys who are "increasingly motivated by profit rather than by the desire to create disruption for its own sake" are someone else. However, we are reminded of the famous line from Pogo, the cartoon strip from the 1960s: "We have met the enemy and he is us." We have, we trust, cited a sufficient number of press reports in the course of the various SWAMI reports to indicate that the bad guys are not just rogue individuals from rogue states, but also governments and the private sector here at home.

The Commission "proposes a dynamic and integrated approach that involves allstakeholders", but is rather thin on specific initiatives with regard to involving users and

[392] European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006]. http://ec.europa.eu/information_society/doc/com2006251.pdf

civil society organisations. It mentions a "structured multi-stakeholder debate" and cites the planned Conference "i2010 – Towards a Ubiquitous European Information Society" being organised by the forthcoming Finnish Presidency, as a contribution to this debate. It also proposes "a seminar reflecting on ways to raise security awareness and strengthen the trust of end-users in the use of electronic networks and information systems". However, given the seriousness and pervasiveness of the risks to security and privacy posed by AmI, we think such initiatives are a good start, but do not go far enough.

Security should be valued as a collective asset. It is a collective good that should in principle be open for everyone. Governments should not leave choices regarding security open to the individual or to the market alone, but impose high standards and invest necessary means. To claim security rights with such a strong collective basis, associations of all kinds are far better placed than individuals. If privacy and security have a future, associations should be allowed to defend them in court.

### 11.2.4 Correcting the lacunae that exist in legislation, regulation

The SWAMI consortium recommends that most of the challenges of new AmI environments be met by legal instruments that do not prohibit new technologies but channel them (transparency tools). In practice, this means data protection and security measures, rather than criminal law prohibitions and heavy administrative burdens. Transparency should be the default position, although some prohibitions referring to the political balances, ethical reasons, or core legal concepts should be also considered in policy discussion.

The SWAMI consortium recommends respect for the diversity and plurality of law-makers within Europe. Without under-estimating the role of the EU institutions, it would not be beneficial to single out these institutions as the sole responsible institutions and lawmakers for the AmI environment. The proposals produced by different stakeholders should be taken into consideration and they should be actively involved in policy discussions. Development of case law should also be closely observed.

In initiatives leading to standardisation of technical specifications for RFIDs, as well as any other similar technology, data protection concerns should be reflected. Privacy assessment of each particular RFID application could be a legally binding obligation

Development of a participatory impact assessment procedure would allow stakeholders to quickly identify and react to any negative features of technology.

A legal framework for sharing knowledge from AmI-generated profiles should be developed, as well as legal protection of technical solutions enabling such information management. A legal framework is needed to cover automated protocols for policy negotiations as well as automated schemes that imply the consent of the data subject. The legal framework should cover situations wherein the explicit consent of the data subject for each collection of data is replaced by a "consent" given by an intelligent agent.

It is necessary to consider development of legal rules with regard to issues that are specific to AmI. In that respect, we propose that legal schemes be developed for digital territories as an important safeguard of privacy in the digital world of AmI. Especially, we propose to

protect such territories against unlawful and unnecessary interference. The specific legal schemes would also be necessary to address the use of software agents and PETs.

The consumer should always be aware of any technological measures embedded in any product he purchases, and restrictions in use of such product as a consequence of technological protection. Product warnings and consumer notifications should always be in place, and should serve to raise consumer awareness about the DRM, RFID and any other technologies having similar impacts.

The right to information (manageable by intelligent agents) is not only a safeguard of consumer rights, but also a privacy safeguard. Thus, we think the individual should have access to information, in both human and machine-readable form, possibly facilitated by use of user-friendly information notices.

Effective liability rules, facilitating proof and empowering individuals (via e.g. representative actions, reversing the burden of poof, strict liability rules), can have a big impact in enforcement of legal provisions. Further examination of such issues is merited.

With regard to the jurisdiction and applicable law, better clarity and legal certainty would be desirable. The Commission should consider a departure from the territorial criterion currently used in private international law towards a personal criterion based on the habitual residence of the consumer, especially since personal data are linked with an identity and a state of a data subject (issues which are regulated by the national law of the person).

The biggest weakness in enforcement of rights is the limitation of any European rules to Member States only, or to countries that have signed international conventions (Cyber crime convention). Clearly, IT and AmI have global dimensions. International co-operation in developing and enforcing the legal framework is necessary. Therefore, the development of a more comprehensive international co-operation framework that would take AmI technologies and capabilities into account is quite urgent.[393]

### 11.2.5 Socio-economic measures

The Commission should consider whether new emerging AmI services should be provided to all in the context of an updated universal services directive. Some services (e.g., emergency services) could be provided free of charge or as part of social security schemes.

## 11.3 Recommendations for the Member States

In the procurement of ICT products, emphasis should be given to critical issues such as security and trustworthiness.

[393] Ofcom, the UK communications regulator, echoes our conclusion with regard to today's Internet: "Effective consumer protection on the internet requires more significant levels of international cooperation than currently exist." Ofcom, *Online protection: A survey of consumer, industry and regulatory mechanisms and systems*, Office of Communications, London, 21 June 2006, p. 4.
http://www.ofcom.org.uk/research/technology/onlineprotection/report.pdf

Member States should consider introducing legislative prohibitions on the admissibility (or general acceptance of the exclusionary rule) of evidence obtained through privacy and/or data protection law infringements.

Appropriate authorities (e.g., the Data Protection Officer) should control and authorise applications of implants after the assessment of the particular circumstances in each case. When an implant enables tracking of people, people should have the possibility to disconnect the implant at any given moment and they should have the possibility to be informed when a (distant) communication (e.g., through RFID) is taking place.

We agree with the European Group on Ethics in Science and New Technologies that irreversible ICT implants should not be used, except for medical purposes. Further research on the long-term impact of ICT implants is also recommended.[394]

In addition to and in line with the right to remain anonymous goes the use of anonymous and pseudonymous credentials, accompanied by unlinkability in certain situations (e.g., e-commerce). Some reconciliation may be necessary between privacy requirements and accountability requirements, for example, in e-commerce. In fact, such mechanisms should always be foreseen when disclosing someone's identity or when linking information is not necessary. Such necessity should not be easily assumed, and in every circumstance more privacy-friendly technological solutions should be sought.[395] However, the use of anonymity should be well balanced. To avoid its misuse, digital anonymity could be further legally regulated, especially stating when it is not appropriate.[396]

Governments that have not yet done so should ratify the Cybercrime Convention. A "revision" mechanism would be desirable so that signatories could negotiate and include in the convention definitions of new, emerging cybercrimes. Specific provisions criminalising identity theft and (some forms of) unsolicited communication could be included within the scope of the convention.

A means to prevent data laundering could be an obligation imposed on those who buy or otherwise acquire databases, profiles and vast amounts of personal data, to check diligently the legal origin of the data. If the buyer does not check the origin and/or the legality of the databases and profiles, he could be considered equal to a receiver of stolen goods and thus held liable for illegal data processing. An obligation could also be created which would require buyers to notify the national data protection officers when personal data(bases) are acquired. Persons or companies involved or assisting in data laundering could be made subject to criminal sanctions.

Governments could fundamentally contribute to the development of good standards by increasing technical regulations, by financing and co-operating in research that leads to standards and by imposing taxes on non-standardised goods and services.

---

[394] European Group on Ethics in Science and New Technologies, "Ethical Aspects of ICT Implants in the Human Body", Opinion to the Commission, 16 March 2005.
http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf

[395] Leenes, Ronald. Koops, Bert-Jan., "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, p.37

[396] Compare Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society), Deliverable D3.2, July 2005, p. 35-36,. http://www.fidis.net

Improving awareness and education should be the responsibility of Member States and/or regional or local authorities (following the subsidiarity principle).

## 11.4 RECOMMENDATIONS FOR INDUSTRY

An approach to alleviate concerns about latent operations and data misuse, thus reducing distrust, is to enhance transparency by effectively informing users about system procedures, purposes and responsibilities. Any networked device, particularly those used by consumer-citizens should come with a privacy warning much like the warnings on tobacco products.

All employees should always be clearly informed about the employer's employee surveillance policy (when and where surveillance is taking place, what use is made of surveillance data, what information is collected, how long it is stored, what are the (procedural) rights of the employees when personal data are to be used as evidence, etc.).

The International Organization for Standardization (ISO) has developed helpful standards and evaluation criteria relevant for IT privacy and security including, most notably, the ISO 15408 and ISO 17799 standards.

Industrial organisations and leaders should highlight the value of ISO certification processes and established codes of practice.

Organisations that compile databases with personal data (even if such compilation is incidental to their primary lines of business) should state on their websites and on product information to what extent they are compliant with ISO 17799 and/or how they have implemented the standard. An organisation could also mention to what extent they follow other guidelines dealing with privacy and security, such as those produced by the OECD.

Those designing AmI networks should ensure that the networks have features that enable effective audits.

Industry should expend less effort on fighting new regulations and more effort on involving stakeholders in the assessment and management of risks to privacy, identity, trust, security and inclusiveness. Involving stakeholders at an early stage will minimise downstream risks.

With respect to use of key technologies of Ambient Intelligence (such as networking of devices and objects, location tracking, authentication etc), manufacturers, suppliers and network operators must do their utmost to avoid negative impacts of new technologies and the bad publicity that follows as a consequence. This will best be done by involving privacy advocates and public interest groups at an early stage in the development of new technologies, especially in actively seeking their views about possible impacts and how such impacts are best addressed.

Engineers and others should not regard technology as "neutral". New technologies often raise policy issues, and this is certainly true of ambient intelligence. AmI offers great benefits, but the risk of not adequately addressing public concerns could mean delays in

implementing the technologies, a lack of public support for taxpayer-funded research and vociferous protests by privacy protection advocates.

As interoperability is a precondition for AmI, programs should be developed so that they are interoperable with each other. That implies a need for new standards applicable to AmI. However, AmI may lead to limitations on exclusive intellectual property rights. Broader scope of the decompilation right would be desirable.

Achieving worldwide interoperability based on standards could also lead to a narrowing of the digital divide. Assistance to the countries and societies that cannot afford to comply with standards developed by the rich and technologically advanced countries is desirable and may be necessary.

## 11.5 Recommendations for civil society organisations

An alternative to peer-rating systems are credibility-rating systems based on the assessment of trusted and independent institutions, such as library associations, consumer groups or other professional associations with widely acknowledged expertise within their respective domains. Ratings should be based on systematic assessments against clearly defined quality standards.

Consumer associations and other civil society organisations (CSOs) could play a useful role as a mediator between service providers and individual consumers and, more particularly, in forcing the development of service contracts (whether real or implicit) between the service provider and the individual consumer. Consumer organisations could leverage their negotiating position through the use of the media or other means of communication with their members. CSOs could position themselves closer to the industry vanguard as represented in platforms such as ARTEMIS by becoming members of such platforms themselves. Within these platforms, CSOs could encourage industry to develop "best practices" in terms of provision of services to consumers.

## 11.6 Recommendations for academia

Institutes of higher education should ensure that courses in ICT-relevant disciplines cover the following content:

- impacts of ICT on society,
- knowledge from technology assessment or from "impact and design research", which has come into being in the field of computing,
- promotion of awareness of development potential for health and the environment in the development phase of new technologies.

This content should, where possible, be integrated into existing school subjects, step by step. The focus should be on longer-term principles, and shorter-lived phenomena should be included only where they provide a clear example of a general principle. This measure requires several individual measures, including the incorporation of these issues into revised curricula and the further training of teaching staff.

Consumers need to be educated about the privacy ramifications arising from virtually any transaction in which they are engaged. An education campaign should be targeted at different segments of the population. Targeting school-age children should be included in any such campaign.

Universities should (continue to) participate in the development of technological safeguards, such as privacy and security protection in networks (including mobile, ad-hoc and sensor networks, as well as personal area networks), in personal devices and in smart spaces, in identity management systems and in developing technological means to minimise the digital divide (such as user interfaces for all, language translation tools, e-learning methods).

## 11.7 RECOMMENDATIONS FOR INDIVIDUALS

Users cannot be innocent bystanders and expect others to look after their interests with regard to privacy and security aspects of the emerging AmI world. We concur with the OECD when it says "Participants [including individual users] should be aware of the need for security of information systems and networks and what they can do to enhance security… Participants should be aware of the … good practices that they can implement to enhance security, and the needs of other participants."[397] At the same time, we recognise that such good advice will not (cannot) be taken onboard by all users, children and the elderly being the most obvious example.

## 11.8 USER CONTROL AND ENFORCEABILITY OF POLICY IN AN ACCESSIBLE MANNER

Throughout the SWAMI project, the partners have faced two problems. One is the trade-off between privacy and security. The comment has been made that an increase in security doesn't necessarily mean a further encroachment on privacy – indeed, security is necessary to protect personal data and our privacy: Networks must be secure, our personal devices, reliable, dependable and trust-worthy. But security is a multi-faceted term, with many dimensions. Our concern in the context of our first problem is where AmI technology is used to help protect society against criminals, terrorists and other miscreants who seek to exploit our personal data in questionable or wrongful ways.

In this latter sense, we are of the view that in an ambient intelligence world, an increase in security most likely *will* encroach upon our privacy. Surveillance cameras will continue to proliferate. We can assume that, whatever the law is, whatever privacy protections government and business *say* they honour, our telecommunications, e-mails and Internet usage will be monitored to increasing degrees. The same will be true of our interfaces with the world of ambient intelligence. The products we buy and use will be linked to us. Personal data will be mined, linked and processed, traded, shared and sold. Many such practices will be unjustified and will violate our rights and civil liberties. We assume or should assume that those encroaching upon our rights and civil liberties will be not only criminals, but (supposedly) legitimate businesses and governments. Even so, the majority of the population may be willing to accept such encroachments because they are genuinely

[397] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD, Paris, 2002, p. 10.

concerned about their own security, that of their family and fellow citizens. The so-called war on terror has undoubtedly provided fertile ground for acceptance.[398]

In an AmI world, we can expect to see a direct trade-off between privacy and security, where the latter refers to the safety of the individual and/or especially the community or society in which he or she lives. And we can assume that gains in security will be made at the expense of losses in privacy.[399] We do not see an easy solution to this problem: indeed, there may not be any. Perhaps the most we can hope for is that unjustified encroachments, abuses and violations will come to light and that offenders will be prosecuted. Coupled with this unhappy prospect is the need for users to be aware, to be vigilant at all times when and where their privacy is put at risk or might be at risk and what users can do, individually and collectively, to minimise those risks. We trust that the safeguards we have suggested in this report can go some distance towards minimising those risks.

The second problem lies in the trade-off between restricting the availability of personal data and personalisation of services. Many of the benefits of AmI lie in the availability of such data in order to personalise services. The greater the restrictions on such data, the greater is the risk that we will not enjoy the full benefits offered by AmI.[400] The restrictions on such data may be imposed by law or by the individual or even by model corporate citizens. Government and, especially, corporate service providers will inevitably want as much personal data as they can get in order to personalise services as much as possible. However, the law may set some limits on how much they can get and users with their personal devices and privacy-enhancing technologies may also set some limits. Where these limits are set partly depends on how much confidence or trust we (individually and collectively) may have in AmI networks (or any network for that matter). If we were confident in the security (in the first sense of the term mentioned above) of the networks and our devices and the software that drives them, then we might be willing to extend those limits and accordingly enjoy greater benefits from AmI. But breaches in networks and software are a daily occurrence today and as networks become increasingly interconnected and complex, we can (should) assume that breaches will continue to plague us for the foreseeable future. Theoretically, it might be possible to solve or at least greater reduce the risk of breaches in security, but then we run up against the human dimension of our first conundrum. Even if it is possible to build totally secure networks and services, how much trust are we willing to extend to governments and businesses or anyone that they will respect our privacy and not abuse it? Unfortunately, even if technology could be made reliable and secure, the prospect of changing human behaviour is even less promising.

Given the problems, the best prospect for ensuring user control and enforceability of policy in an accessible manner is to involve the user in the process of formulating policy, to

---

[398] "Since the 2001 terror attacks, a slim majority of the American public has favored protecting security over preserving civil liberties, according to opinion pollsters." Mohammed, Arshad, and Sara Kehaulani Goo, "Government Increasingly Turning to Data Mining", *The Washington Post*, 15 June 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html

[399] Security expert Bruce Schneier has commented, "We're not trading privacy for security; we're giving up privacy and getting no security in return." Schneier, Bruce, "Why Data Mining Won't Stop Terror", Wired News, 9 March 2005. http://www.schneier.com/essay-108.html

[400] The point is made in _as, Johann, "Privacy in Pervasive Computing Environments – A Contradiction in Terms?", *IEEE Technology and Society Magazine*, Volume 24, Issue 1, Spring 2005, pp 24-33. http://www-personal.si.umich.edu/~rfrost/courses/SI110/paper_support/Cas,%20Privacy%20and%20Ubiquity.pdf

achieve so far as possible consensus on a policy development to which the user has contributed. The user should be encouraged to express his or her views, to provide information that might be helpful to other stakeholders. The views of all stakeholders (users) should be carefully considered and they should be informed to what extent they have been taken into account or, if they haven't been, then why not.

Needless to say, user control and enforceability of policy will work best in a transparent decision-making process, and we commend, as stated above, a formalised risk assessment – risk management process to that end.

In addition, we think industry initiatives, notably that of ARTEMIS platform, would be more successful if user concerns were recognised and taken into account through the participation of civil society organisations. Issues of privacy, identity management and digital divide should be considered by all working groups in academia and industry (which now is not the case) and that industry participants should not see regulatory concerns as barriers to be overcome, but as opportunities to ensure user acceptance of AmI. As the Commission has generally been promoting platforms as a means of strengthening European success in key areas, so the Commission could take the initiative to encourage the ARTEMIS participants to establish a working group devoted to the policy issues that have been the focus of the SWAMI project. This recommendation could also be applicable to other EC-inspired platforms.

## 11.9 Concluding remarks – The top six

This report has identified many threats and vulnerabilities and many safeguards for dealing with them. It does not pretend to be comprehensive. Our recommendations are not to be found only in this chapter (although it contains the main ones), but also in the chapter on safeguards.

Even though our report does not pretend to be comprehensive, perhaps we have identified too many safeguards or made too many recommendations, at least, in the sense that we have our doubts about how many officials in the Commission or in Member States or in industry and so on are going to systematically go through our proposed safeguards and recommendations, consider them and decide which are feasible, sensible or implementable.

We hope all of the stakeholder groups mentioned in this report do, at least, consider all of our safeguards and recommendations, but in the event that so many seem daunting, the SWAMI partners decided to prioritise them and the following our top six recommendations.

1. The Commission, together with Member States, perhaps under the auspices of ENISA should initiate a formalised risk assessment / risk management process with regard to the risks posed by AmI to security and privacy. We recommend that the assessment and decision-making process be open, transparent and inclusive, that stakeholder groups be identified and contacted and encouraged to take part in the process. Individuals should also be given an opportunity to express their views. Such a process could be initiated by means of a green paper on the risks to security and privacy in an AmI world. Whatever the outcome of the process, we recommend that the risk assessment be undertaken again (and again) in the future with some regularity, the periodicity of which might depend on the

rapidity with which AmI is deployed (bearing in mind that the technologies for AmI are already being developed and deployed).

We also recommend that the precautionary approach be taken into account when developing and deploying new technologies. Such an exercise might be considered as a legal obligation.

2. The Commission and Member States should invest in an awareness campaign specifically focused on AmI, the purpose of which would be to explain to all stakeholders, but especially the public that AmI is on its way, that it offers great benefits, but also poses certain security and privacy issues. There are many ways of raising awareness (through education, the media, etc), but to give this recommendation some specific focus, we recommend that Member States hold an annual national contests which would offer some form of recognition to the best product or service offering privacy and security protection. We recommend a run-off at European level. This could be a counterpoint to the notorious bad publicity that ambient intelligence (especially RFID applications) has received in recent years.[401]

Any such campaign targeted at informing the public about ambient intelligence services and to inspire trust should involve *all* stakeholders and any such competition should be judged by independent evaluators.

3. The Commission and Member States should review carefully this report and, especially, section 10.3, to address the inadequacies and lacunae in the existing legal and regulatory framework with respect to AmI.[402] Law is only one of the available tools for regulating behaviour, in addition to social norms, market rules and the "code", i.e., the architecture of the technology (e.g. cyberspace, ambient intelligence, mobile telephony…). The law can be a regulator on its own, but it can also regulate via influencing the "code" and other modalities of regulation.

The SWAMI consortium strongly recommends respecting this pluralism of modalities of regulation. In order to tackle the identified problems effectively, it is necessary to consider different approaches simultaneously.

4. The SWAMI consortium recommends that most of the challenges of new AmI environments be met by legal instruments that do not prohibit new technological developments, but channel them (such as by data protection and security measures). Transparency should be the default position, although some prohibitions referring to the political balances, ethical reasons or core legal concepts should be also considered in policy discussion. Focusing on concrete technologies rather than trying to produce general solutions seem to be more appropriate for AmI, an environment that adapts and responds to the changes of context, and in which privacy and other legal issues are also context-

[401] RFID technologies and their promoters have received Big Brother Awards in various countries world wide. See e.g. http://bigbrotherawards.de/2003/.cop/; http://www.edri.org/edrigram/number4.3/frenchbba?PHPSESSID=a08c4d85ac916daab3d8660a1d377dd8; http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-187899; http://www.bigbrotherawards.cz/en/winners_2005.html

[402] We also encourage a careful review of the SWAMI D3 report which provides a still more detailed set of safeguards.

dependent. Thus, in developing policy options, one should focus on the concrete technologies, and apply channelling and prohibitive approaches accordingly.

5. The biggest weakness in enforcement of rights is the limitation of any European rule to Member States only, or to countries which have signed international conventions such as the Cyber Crime Convention). Clearly, ICTs and AmI have global dimensions. International cooperation in developing and enforcing the legal framework is necessary. Therefore, the Commission and Member States should be proactive in the development of a more comprehensive international co-operation framework that would take AmI technologies and capabilities into account as a matter of urgency.

6. The European Commission should ensure that projects that it funds take questions of privacy, security and trust into account. Research programmes should contain a project line of accompanying measures covering the societal impact. Currently, EC calls say that project participants must conform to relevant EU legislation, inter alia, the data protection directive (95/46/EC). It is, of course, necessary that project participants (or any third party funded by the EC) conform to EU legislation, but we think the Commission should be more demanding – i.e., it should require those it funds to specifically speculate what privacy or security impacts might arise from their projects and what measures should be taken to address those. In other words, simply conforming to legislation is not enough. Project participants must be asked to foresee or even to speculate what privacy or security implications their projects *might* have. By the same token, the EC proposal and tender evaluators should also be asked to evaluate project proposals and tenders from the same optic. We recommend that Member States adopt a similar approach. We would like to especially emphasise the importance of funding research on technological safeguards for protecting privacy and enhancing security and for overcoming the digital divide. If technology does not provide solutions for human-technology interfaces for all, or for user-friendly security, other safeguards will not be able to solve the problem. We suggest that among technological safeguards research on intelligent algorithms is especially important.

As a final, parting comment for this report, the SWAMI partners believe that, sooner or later, we will live in a world of ambient intelligence. For ambient intelligence to be a success story, in human terms, according to democratic principles, and not to be an Orwellian world, all stakeholders must be cognisant of the threats and vulnerabilities and work together to ensure adequate safeguards exist. Certainly, industry should become more active in creating applications that are secure and privacy enhancing since this is the major way to create consumer trust and make ambient intelligence fruitful to *all* participants. Industry should not view privacy, security, identity, trust, and inclusion issues as regulatory barriers to be overcome. Rather, they should regard such measures as necessary, justified and, in the end, crucial to ensuring that their fellow citizens will use ambient intelligence technologies and services. In the meantime, we encourage all stakeholders to be vigilant.

# 12 REFERENCES

## 12.1 GENERAL


Aarts, E., R. Harwig and M. Schuurmans, "Ambient Intelligence", in P. Denning, *The Invisible Future: The Seamless Integration of Technology in Everyday Life*, McGraw-Hill, New York, 2002.

Åkesson, K.-P., J. Humble, A. Crabtree, A. and A. Bullock, *Usage and Development Scenarios for the Tangible Toolbox*, ACCORD Deliverable D1.3, Swedish Institute of Computer Science, Kista, 2001.

Alahuhta, P., M. Jurvansuu and H. Pentikäinen, "Roadmap for network technologies and service", *Tekes Technology Review* 162/2004, Tekes, Helsinki, 2004

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, 2001.

Andrews, S., *Privacy and human rights 2002*, produced by the Electronic Privacy Information Center (EPIC), Washington, D.C. and *Privacy International*, London, 2002.
*http://www.privacyinternational.org/survey/phr2002/*

*ARTEMIS Strategic Research Agenda*, First Edition, March 2006.
http://www.artemis-office.org/DotNetNuke/PressCorner/tabid/89/Default.aspx

Aschmoneit, P. and M. Höbig, *Context-Aware Collaborative Environments for Next Generation Business Networks: Scenario Document*, COCONET deliverable D 2.2, Telematica Institute, Enschede, 2002.
http://www.mosaic-network.org/library/scenarios.html

Bauer M., M. Meints and M. Hansen (eds.), *Structured Overview on Prototypes and Concepts of Identity Management Systems*, FIDIS (Future of Identity in the Information Society) Deliverable D3.1, September 2005.

Becher, A., Z. Benenson and M. Dornseif, "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks", Third International Conference on Security in Pervasive Computing, York, UK, April 2006, pp. 104-118.

Beslay, L., and H. Hakala, "Digital Territory: Bubbles", draft version available at http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf

Beslay, L. & Y. Punie, "The Virtual Residence: Identity, Privacy and Security", *Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview*, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003.
http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html

Bolle, R.M., J.H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior, *Guide to Biometrics*, New York, Springer, 2004.

Borking, J., "RFID Security, Data Protection & Privacy, Health and Safety Issues", presentation made during European Commission Consultation on RFID, Brussels, 17 May 2006.

Brey, Philip, "Freedom and privacy in Ambient Intelligence", *Ethics and Information Technology*, Vol. 7, No. 3, 2005.

Brownsword, Roger, "Code, control, and choice: Why East is East and West is West", *Legal Studies*, Vol. 25 No 1, March 2005, pp. 1-21.

Burnett, R. and P.D. Marshall, *Web Theory: An Introduction*, Routledge, London, 2002.

Cabrera Giráldez, M., and C. Rodríguez Casal, "The role of Ambient Intelligence in the Social Integration of the Elderly" in G. Riva, G., F. Vatalaro, et al. (eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction*, IOS Press (Studies in New Technologies and Practices in Communication, 6), Amsterdam, 2005, pp. 265-280.

Carr, S., "Wireless tagging in hospitals is 'inevitable': Prepare to be chipped...", silicon.com, 7 December 2004.
http://hardware.silicon.com/storage/0,39024649,39126387,00.htm

_as, Johann, "Privacy in Pervasive Computing Environments – A Contradiction in Terms?", *Technology and Society Magazine*, IEEE, Volume 24, Issue 1, Spring 2005, pp. 24-33.

CDT (Centre for democracy and technology) Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology**,** Interim Draft, 1 May 2006, http://www.cdt.org/privacy/20060501rfid-best-practices.php

Claes, Erik, Anthony Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Intersentia, Antwerp/Oxford, 2006.

Clarke, R., "Information Technology and Dataveillance", *Communications of the ACM*, 31(5), May 1988, pp. 498-512.

Creese, S., M. Goldsmith and I. Zakiuddin, "Authentication in Pervasive Computing", First International Conference on Security in Pervasive Computing, Boppard, Germany, 12-14 March 2003, pp. 116-129.

Custers, B., *The Power of Knowledge, Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen, 2004.

Da Costa, O., M. Boden, Y. Punie, M. Zappacosta, "Science and Technology Roadmapping from Industry to Public Policy", in *The IPTS Report* 73, 2003.

De Hert, P., "De soevereiniteit van de mensenrechten: aantasting door de uitlevering en het bewijsrecht" [Sovereignty of human rights: threats created by the law of extradition and by

the law of evidence], Panopticon, *Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, Vol. 25, No. 3, 2004, pp. 229-238.

De Hert, P., *Biometrics: legal issues and implications*, Background paper for the Institute of Prospective Technological Studies, EC – JRC, Sevilla, January 2005. http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf

De Hert, P., "What are the risks and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection',* No. 1. ww.vub.ac.be/LSTS/pub/Dehert/006.pdf

De Hert, P., "European Data Protection and E-Commerce: Trust Enhancing?", in J.E.J. Prins, P.M.A. Ribbers, H.C.A. Van Tilborg, A.F.L. Veth & J.G.L. Van Der Wees (eds.), *Trust in Electronic Commerce*, Kluwer Law International, The Hague, 2002, pp. 190-199.

De Hert, P., "What are the risks and what guarantees need to be put in place in view of interoperability of police databases?", Standard Briefing Note 'JHA & Data Protection', No. 1, produced in January 2006 on behalf of the European Parliament, available through http://www.vub.ac.be/LSTS/

De Hert, Paul, & Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in Erik Claes, Anthony Duff & Serge Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, pp. 61-104.

De Hert P. & S. Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence" in *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Institute for Prospective Technological Studies - Joint Research Centre, Seville, July 2003, pp. 111-162. ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf

De Hert, P., & S. Gutwirth, "Interoperability of police databases: an accountable political choice", to be published in *International Review of Law Computers & Technology*, 2006.

De Hert P. & F.P. Ölcer, "Het onschadelijk gemaakte Europees privacybegrip. Implicaties voor de Nederlandse strafrechtspleging" [The notion of privacy made innocent. Implications for criminal procedure], *Strafblad. Het nieuwe tijdschrift voor strafrecht,* Vol. 2, No 2, 2004, pp. 115-134.

Desai, M.S., J. Oghen and T.C. Richards, "Information Technology Litigation and Software Failure", *The Journal of Information, Law & Technology*, 2002 (2). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/desai/

Drees, Caroline, "Civil liberties debate leaves much of America cold", Reuters, published in *The Washington Post*, 18 May 2006.

Edler, J., (ed.), "Politikbenchmarking Nachfrageorientierte Innovationspolitik", Progress report No. 99, Office for Technology Assessment at the German Parliament, Berlin, 2006.

Eggermont, L. D. J., Embedded Systems Roadmap 2002: Vision on technology for the future of PROGRESS, STW Technology Foundation/PROGRESS, Utrecht, 2002. www.stw.nl/progress/ESroadmap/index.html

Emiliani, P.L., and C. Stephanidis, "Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities", *IBM Systems Journal* 44, No. 3, 2005, pp. 605-619.

Engberg, Stephan, "Empowerment and Context Security as the route to Growth and Security", SWAMI Final Conference, Brussels, 21-22 March 2006. http://swami.jrc.es.
Espiner, T., "Philips unfurls prototype flexible display", ZDNet UK, http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39216111,00.htm

Espiner, Tom, "Viruses cause most security breaches", ZDNet UK, 28 Feb 2006. http://news.zdnet.co.uk/0,39020330,39254929,00.htm.

Estrin, Deborah (ed.), *Embedded, Everywhere*: A Research Agenda for Networked Systems of Embedded Computers, National Academy Press, Washington, D.C., 2001.

European Commission, Work Programme for the specific programme for research, technological development and demonstration: "Integrating and strengthening the European Research Area": Specific activity covering policy-orientated research under "Policy support and anticipating scientific and technological needs" (SSP Call 3), Brussels, 2003.

European Commission, *Technology Platforms: from Definition to Implementation of a Common Research Agenda*: Report compiled by a Commission Inter-Service Group on Technology Platforms, Office for Official Publications of the European Communities, Luxembourg, 2004.
http://www.eurogif.org/wimages/Technology_Platforms_21_September_2004.pdf

European Commission, *Science and technology, the key to Europe's future - Guidelines for future European Union policy to support research*, COM(2004) 353 final, Brussels, 2004. ftp://ftp.cordis.lu/pub/era/docs/com2004_353_en.pdf

European Commission, *Report on European Technology Platforms and Joint Technology Initiatives*: Fostering Public-Private R&D Partnerships to Boost Europe's Industrial Competitiveness, Commission Staff Working Document, SEC(2005) 800, Brussels, 2005.

European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006].
http://ec.europa.eu/information_society/doc/com2006251.pdf

European Commission, Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European

databases in the area of Justice and Home Affairs, COM (2005) 597 final, Brussels, 24 November 2005.

European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006].
http://ec.europa.eu/information_society/doc/com2006251.pdf

[European Commission] *Impact Assessment*: Commission Staff Working Document, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the EU Regulatory Framework for electronic communications networks and services, SEC(2006) 817, Brussels, 28 June 2006.
http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/public_consult/review/impactassessment_final.pdf.

European Data Protection Supervisor (EDPS), *Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability* (COM (2005) 490 final), Brussels, 28 February 2006.
http://www.edps.eu.int/legislation/Opinions_A/06-02-28_Opinion_availability_EN.pdf

European Data Protection Supervisor (EDPS), *Opinion* on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM (2004)835 final, *OJ C* 181/27, 23 July 2005.

European Data Protection Supervisor (EDPS), *Comments on the Communication of the Commission on interoperability of European databases*, 10 March 2006.
http://www.edps.eu.int/legislation/Comments/06-03-10_Comments_interoperability_EN.pdf

European Data Protection Supervisor (EDPS), *Annual Report 2005*.
http://www.edps.eu.int/publications/annual_report_en.htm

European Group on Ethics in Science and New Technologies, "Ethical Aspects of ICT Implants in the Human Body", Opinion to the Commission, 16 March 2005.
http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf

Friedewald, Michael, Ralf Lindner & David Wright (eds.), *Threats, Vulnerabilities and Safeguards in Ambient Intelligence*, Deliverable D3, A report of the SWAMI consortium to the European Commission, 3 July 2006.

Friedewald, M., & D. Wright (eds.), *Report on the Final Conference*, Brussels, 21-22 March 2006, SWAMI Deliverable D5, 2006.
http://swami.jrc.es/pages/documents/Deliverable5-ReportonConference.pdf

Friedewald, M., E. Vildjiounaite & D. Wright, *The brave new world of ambient intelligence*, Deliverable D1, A report of the SWAMI consortium to the European Commission under contract 006507, June 2005. http://swami.jrc.es.

Friedewald, Michael, Elene Vildjiounaite, Yves Punie and David Wright, "The Brave New World of Ambient Intelligence: An Analysis of Scenarios Regarding Privacy, Identity and Security Issues", in John A. Clark et al (eds.), *Security in Pervasive Computing*: Proceedings of the Third International Conference, SPC 18-21 April 2006, York, UK, published by Springer-Verlag, Berlin, 2006.

Fule, P., and J.F. Roddick, "Detecting Privacy and Ethical Sensitivity in Data Mining Results" in V. Estivill-Castro (ed.), *Computer Science 2004*, Twenty-Seveth Australasian Computer Science Conference (ACSC2004), Dunedin, New Zealand, January 2004, Australian Computer Society (CRPIT, 26), 2004, pp. 159-166.

Garlan, D., D. Siewiorek, A. Smailagic and P. Steenkiste, "Project Aura: Toward Distraction-Free Pervasive Computing" in *IEEE Pervasive Computing* 21, No. 2, 2002

Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005. http://www.fidis.net

Godet, M., "The art of scenario and strategic planning: tools and pitfalls", *Technological Forecasting and Social Change,* 65, 2000, pp.3-22.

Gavigan, J.P., F. Scapolo, M. Keenan, I. Miles, F. Farhi, D. Lecoq, M. Capriati, T. Di Bartolomeo (eds.), "A practical guide to Regional Foresight", EUR 20128 EN, IPTS, Sevilla, December 2001.

Gehring, R. A., "Software Development, Intellectual Property, and IT Security", *The Journal of Information, Law and Technology*, 1/2003. http://elj.warwick.ac.uk/jilt/03-1/gehring.html.

Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", *Netherlands Comparative Law Association*, 2002, pp. 75-79. http://www.ejcl.org/64/art64-6.html.

Günther, Oliver and Sarah Spiekermann, "RFID and the Perception of Control: The Consumer's View", *Communications of the ACM*, Vol. 48, No. 9, 2005.

Gutwirth, S., "De polyfonie van de democratische rechtsstaat" [The polyphony of the democratic constitutional state] in M. Elchardus (ed.), *Wantrouwen en onbehagen* [Distrust and uneasiness], Balans 14, VUBPress, Brussels, 1998, pp.137-193.

Gutwirth, S., and P. de Hert, "Privacy and Data Protection in a Democratic Constitutional State" in M. Hildebrandt and S. Gutwirth (eds.), *Profiling: Implications for Democracy and Rule of Law*, FIDIS deliverable 7.4, Brussels, 2005. www.fidis.net

Gutwirth, S. & P. De Hert, "Regulating profiling in a democratic constitutional state", to be published in M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen*, forthcoming, Springer Press, Berlin, 2007.

Hansell, Saul, "Increasingly, Internet's Data Trail Leads to Court", *The New York Times*, 4 Feb 2006.

Hansen, Marit and Henry Krasemann (eds.), *Privacy and Identity Management for Europe* – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005. http://www.prime-project.eu.org/public/prime_products/deliverables/

Harmon, Amy, "Lost? Hiding? Your Cellphone Is Keeping Tabs", *The New York Times*, 21 Dec 2003.

Henderson, K., and A. Poulter, "The Distance Selling Directive: Points for Further Revision", *International Review for Law Computers & Technology*, Vol. 16 no. 3, 2002, pp. 289-300.

Hildebrandt M., "Profiling and the Identity of European Citizens" in M. Hildebrandt and S. Gutwirth (eds.), *Profiling: Implications for Democracy and Rule of Law*, FIDIS deliverable 7.4, Brussels, 2005. www.fidis.net

Hildebrandt, M., and J. Backhouse (eds.), *Descriptive analysis and inventory of profiling practices*, FIDIS (Future of Identity in the Information Society) Deliverable D7.2. http://www.fidis.net

Hildebrandt, M., and S. Gutwirth (eds.), *Implications of profiling on democracy and the rule of law*, FIDIS (Future of Identity in the Information Society), Deliverable D7.4, September 2005. http://www.fidis.net.

Hilty, Lorenz, 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.

INDICARE Project, "Content Providers' Guide to Digital Rights Management: Any side effects in using DRM?". www.indicare.org

ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*, First edition, International Organization for Standardization, Geneva, 1999.

ISO/IEC 17799:2005(E), *Information Technology – Security techniques – Code of Practice for Information Security Management*, International Organization for Standardization, Geneva, 2005.

IST Advisory Group, *Ambient Intelligence: From Vision to Reality*. For participation – in society and business, Office for Official Publications of the European Communities, Luxembourg, 2003. http://www.cordis.lu/ist/istag-reports.html

IST Advisory Group, K. Ducatel, M. Bogdanowicz et al., *Scenarios for Ambient Intelligence in 2010*, EUR 19763 EN, EC-JRC, Institute for Prospective Technological Studies (IPTS), Sevilla, 2001. http://www.cordis.lu/ist/istag-reports.html.

ITEA *Technology Roadmap for Software-Intensive Systems*, 2nd edition, Information Technology for European Advancement (ITEA) Office Association, Eindhoven, 2004. www.itea-office.org

Ito, M., A. Iwaya, M. Saito et al., "Smart Furniture: Improvising Ubiquitous Hot-spot Environment" in *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops* (ICDCSW'03), Providence, RI, 19–22 May 2003, IEEE Press, 2003, pp. 48-53.

Jordan, Mary, "Electronic Eye Grows Wider in Britain", *The Washington Post*, 7 January 2006.

Julia-Barcelo, R., and K. J. Koelman, "Intermediary Liability in the E- commerce Directive: So far so Good, But It's not Enough", *Computer Law and Security Report*, Vol. 16, No. 4, 2000, pp. 231-239.

Kaasinen, E., K. Rentto, V. Ikonen and P. Välkkynen, *MIMOSA Initial Usage Scenarios*, MIMOSA Deliverable D1.1, version 1.0, 2004. http://www.mimosa-fp6.com/cgi-bin/WebObjects/MIMOSA.woa/1/wo/g6hDj8CHIFBQDjTQXuNVGM/8.0.5.11.

Kardasiadou, Z., and Z. Talidou, *Report on Legal Issues of RFID Technology*, LEGAL IST (Legal Issues for the Advancement of Information Society Technologies) Deliverable D15, 2006.

Kato, U., T. Hayashi, N. Umeda et al (eds.), *Flying Carpet: Towards the 4th Generation Mobile Communications Systems*, Ver. 2.00, 4th Generation Mobile Communications Committee, 2004. www.mitf.org/public_e/archives/index.html

Kawahara, Y., M. Minami, S. Saruwatari et al, "Challenges and Lessons Learned in Building a Practical Smart Space", in *The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, Boston, MA., 22-26 August 2004, pp. 213- 222.

Kelly, Lisa, "Spyware attacks triple in 2005", *Computing*, 12 Jun 2006 http://www.vnunet.com/computing/news/2158112/spyware-attacks-triple-2005.

Kent, S. T. and L.I. Millett (eds.), *Who Goes There? Authentication Through the Lens of Privacy*. National Academies Press, Washington, DC, 2003

Kent, Stephen T., and Lynette I. Millett (eds.), *IDs--Not That Easy. Questions About Nationwide Identity Systems*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academy Press, Washington, DC, 2002.

Knospe, H., and H. Pohl, "RFID Security", in *Information Security Technical Report* 9, No. 4, 2004, S. 30-41.

Koops, B.J. & M.M. Prinsen, "Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit" ["Glass house, transparent body. A future view on home law and body integrity"], *Nederland Juristenblad*, 12 March 2005, pp. 624-630.

Koorn, R., H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen and J. Borking, "Privacy-Enhancing Technologies. White Paper for Decision-Makers", The Hague, Ministry of the Interior and Kingdom Relations, 2004.
http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

Kravitz, D. W., K.-E. Yeoh and N. So, "Secure Open Systems for Protecting Privacy and Digital Services", in T. Sander (ed.), *Security and Privacy in Digital Rights Management,* ACM CCS-8 Workshop DRM 2001, Philadelphia, 5 Nov 2001, Revised Papers, Springer, Berlin, 2002, pp. 106 – 25.

Krebs, Brian, "Hackers Break Into Computer-Security Firm's Customer Database", *The Washington Post*, 19 Dec 2005.

Krebs, Brian, "Microsoft Releases Windows Malware Stats", *The Washington Post*, 12 June 2006.
http://blog.washingtonpost.com/securityfix/2006/06/microsoft_releases_malware_sta.html

Krebs, Brian, "Invasion of the Computer Snatchers", *The Washington Post*, 19 Feb 2006.

Krim, Jonathan, "Consumers Not Told Of Security Breaches, Data Brokers Admit", *The Washington Post*, 14 April 2005

Krim, Jonathan, "Data on 3,000 Consumers Stolen With Computer", *The Washington Post*, 9 November 2005

Krikke, J., "T-Engine: Japan's Ubiquitous Computing Architecture Is Ready for Prime Time", in *Pervasive Computing* 4, No. 2, 2005, pp. 4-9.

Kruger, Danny, *Access Denied? Preventing Information Exclusion*, Demos, London, 1998.

Lahlou, S., and F. Jegou, "European Disappearing Computer Privacy Design Guideslines V1", Ambient Agora Deliverable D15.4, Electricité de France, Clamart, 2003. http://www.ambient-agoras.org/downloads/D15[1].4_-_Privacy_Design_Guidelines.pdf.

Lahlou, Saadi, Marc Langheinrich and Carsten Rocker, "Privacy and Trust Issues with Invisible Computers", *Communications of the ACM*, Vol. 48 No. 3, March 2005.

Langheinrich, M., "The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects", Paper presented at the Designing for Privacy Workshop, DC Tales Conference, Santorini, Greece, 2003.

Langheinrich, M., "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems", in G. D. Abowd, B. Brumitt and S. A. Shafer (eds.), *Proceedings of the Third International Conference on Ubiquitous Computing* (Ubicomp 2001), Springer-Verlag, Berlin, 2001, pp. 273-91.

Leenes, R., and B.J. Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers & Technology*, Vol. 19, No 3, 2005.

Lemos, Robert, "Cybersecurity contests go national", *The Register*, 5 June 2006. http://www.theregister.co.uk/2006/06/05/security_contests/ This article originally appeared at *SecurityFocus*. http://www.securityfocus.com/news/11394

Lessig, Lawrence, "The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 133, 1999, pp. 501-546.

Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

Leyden, John, "Hackers cost UK.biz billions", *The Register*, 28 April 2004. http://www.theregister.co.uk/2004/04/28/dti_security_survey/

Maghiros, I., Y. Punie, S. Delaitre. et al., *Biometrics at the Frontiers: Assessing the Impact on Society*, Study commissioned by the LIBE committee of the European Parliament, EC – DG Joint Research Centre, EUR 21585 EN, Institute for Prospective Technological Studies (IPTS), Seville, 2005. http://www.jrc.es/home/pages/detail.cfm?prs=1235.

Magnus, U., and H.W. Micklitz, *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. http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportabc_en.pdf http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf

Masera, M. and R. Bloomfeld, *A Dependability Roadmap for the Information Society in Europe*, AMSD Delilverable D1.1, 2003. https://rami.jrc.it/roadmaps/amsd.

Massini, E.H. & J. M. Vasquez, "Scenarios as seen from a human and social perspective", *Technological Forecasting and Social Change*, 65, 2000, pp.49-66.

Meints, M., "AmI – The European Perspective on Data Protection Legislation and Privacy Policies", presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006. http://swami.jrc.es/pages/deliverables.htm

Michahelles, F., P. Matter, A. Schmidt, B. Schiele, "Applying Wearable Sensors to Avalanche Rescue: First Experiences with a Novel Avalanche Beacon" in *Computers & Graphics* 27, No. 6, 2003, pp. 839-847.

Miles, I., M. Keenan and J. Kaivo-Oja, "Handbook of Knowledge Society Foresight", European Foundation for the Improvement of Living and Working Conditions, Dublin, 2003. This handbook is available in electronic format only: www.eurofound.eu.int.

Mohammed, Arshad, "Record Fine for Data Breach", *The Washington Post*, 27 January 2006.

Mohammed, Arshad, and Sara Kehaulani Goo, "Government Increasingly Turning to Data Mining", *The Washington Post*, 15 June 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html

Molas-Gallart, J., "Government Policies and Complex Product Systems: The Case of Defence Standards and Procurement", *International Journal of Aerospace Management*, vol. 1, no. 3, 2001, pp. 268-80.

Moores, T., "Do Consumers Understand the Role of Privacy Seals in E-Commerce?", *Communications of the ACM*, Vol. 48, no. 3, 2005, pp. 86-91.

MPHPT, Information and Communications in Japan: *Building a Ubiquitous Network Society that Spreads Throughout the World*, White Paper, Ministry of Public Management Home Affairs Posts and Telecommunications of Japan, Economic Research Office, General Policy Division, Tokyo, 2004.
http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2004/2004-index.html

Müller G. and S. Wohlgemuth (eds.), *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, May 2005. http://www.fidis.net.

Nissenbaum, H., "Privacy as Contextual Integrity", in *Washington Law Review* 79, No. 1, 2004, pp. 101-139.

Norris, Pippa, *Digital divide: Civic engagement, information poverty, and the Internet worldwide*, Cambridge University Press, Cambridge, 2001.

O'Brien, Timothy L., "Identity Theft Is Epidemic. Can It Be Stopped?", *The New York Times*, 24 Oct 2004.

*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Co-operation and Development, Paris, 2001.

*OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,* Organisation for Economic Co-operation and Development, Paris, 2002.

OECD, *Emerging Risks in the 21st Century*, Paris, 2003.

OECD, *Report on Disclosure Issues Related to the Use of Copy Control and Digital Rights Management Technologies*, DSTI/CP(2005)15/FINAL, 2006.
https://www.oecd.org/dataoecd/47/31/36546422.pdf.

Ofcom, Online protection: A survey of consumer, industry and regulatory mechanisms and systems, 21 June 2006.
http://www.ofcom.org.uk/research/technology/onlineprotection/report.pdf

O'Harrow, Robert, *No Place to Hide*, Simon & Schuster, New York, 2005.

Olsen T., T. Mahler, et al, "Privacy – Identity Management, Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", LEGAL IST: LEGAL Issues for the Advancement of Information Society Technologies, Deliverable D11, 2005. See LEGAL IST website
http://193.72.209.176/default.asp?P=369&obj=P1076

Orr, R. J., R. Raymond, J. Berman and F. Seay, "A System for Finding Frequently Lost Objects in the Home", *Technical Report 99*-24, Graphics, Visualization, and Usability Center, Georgia Tech, 1999.

Paciga, M. & H. Lutfiyya, "Herecast: An open infrastructure for location-based services using WiFi, Wireless And Mobile Computing, Networking And Communications", WiMob'2005, IEEE International Conference, pp.21-28, 2005.

Palmas, G., N. Tsapatsoulis, B. Apolloni et al., *Generic Artefacts Specification and Acceptance Criteria*, Oresteia Deliverable D01, STMicroelectronics s.r.l., Milan, 2001.

Pennington, R., H. D. Wilcox and V. Grover, "The Role of System Trust in Business-to-Consumer Transactions", *Journal of Management Information System*, vol. 20, no. 3, 2004, pp. 197-226.

Perri 6 and Ben Jupp, *Divided by information? The "digital divide" and the implications of the new meritocracy*, Demos, London, 2001.

Pfitzmann, Andreas, "Anonymity, unobservability, pseudonymity and identity management requirements for an AmI world", SWAMI Final Conference, Brussels, 21-22 March 2006. http://swami.jrc.es.

Pfizmann, A. and M. Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology,* Version v0.27, 20 Feb. 2006. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

Pfitzmann, A. and M. Kohntopp, "Striking a Balance between Cyber-Crime and Privacy", *IPTS Report* 57, EC-JRC, Seville, Sept 2001.
http://www.jrc.es/home/report/english/articles/vol57/welcome.htm

Poulsen, Kevin, "Traffic Hackers Hit Red Light", *Wired News*, 12 August 2005.
http://www.wired.com/news/technology/0,1282,68507,00.html

Prins, J.E.J., "The Propertization of Personal Data and Identities", *Electronic Journal of Comparative Law*, vol. 8.3, October 2004. http://www.ejcl.org

Prins, J. E. J., and M.H.M. Schellekens, "Fighting Untrustworthy Internet Content: In Search of Regulatory Scenarios", *Information Polity*, vol.10, 2005, pp. 129-39.

Punie, Y., S. Delaitre, I. Maghiros and D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission, November 2005.
http://swami.jrc.es.

Ranneberg, K., "Multilateral Security: A Concept and Examples for Balanced Security", ACM New Security Paradigms Workshop, September 2000, 151-162.

Reed, Ch., and A. Welterveden, "Liability", in Ch. Reed and J. Angel (eds.), *ComputerLaw*, London 2000.

Resnick, P. and R. Zeckhauser, "Trust Among Strangers in Internet Transactions: Empircal Analysis of eBay's Reputation System", in Michael R. Baye (ed.), *The Economics of the Internet and E-Commerce*, Vol. 11 of *Advances in Applied Microeconomics*, JAI Press, Amsterdam, 2002, pp. 127-157.

Resnick, P., R. Zeckhauser, E. Friedman and K. Kuwabara,. "Reputation Systems: Facilitating Trust in Internet Interactions", *Communications of the ACM*, 43(12), 2000, pp. 45-48. http://www.si.umich.edu/~presnick/papers/cacm00/reputations.pdf

Richtel, Matt, "Suddenly, an Industry Is All Ears", *The New York Times*, 4 March 2006.

Sachinopoulou, A., S. Mäkelä, S. Järvinen, et al., "Personal video retrieval and browsing for mobile users" in *17th International Symposium Electronic Imaging Science and Technology*, San José, CA, 16-20 January 2005.

Samuelson, P., "Privacy As Intellectual Property?", *Stanford Law Review*, Vol. 52, 2000.

Savidis, A., S. Lalis, A. Karypidis et al, *Report on Key Reference Scenarios*, 2WEAR Deliverable D1, Foundation for Research and Technology Hellas, Institute of Computer Science, Heraklion, 2001.

Schneider, F. B. (ed.), *Trust in Cyberspace*, National Academy Press, Washington, D.C., 1999.

Schneier, B., "Customers, Passwords, and Web Sites", in *IEEE Security & Privacy Magazine* 2, No. 5, 2004.

Schneier, Bruce, "Identification and Security", *Crypto-Gram Newsletter*, 15 Feb 2004. http://www.schneier.com/crypto-gram-back.html.

Schneier, Bruce, "National ID Cards", *Crypto-Gram Newsletter*, 15 Apr 2004. http://www.schneier.com/crypto-gram-back.html

Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick, *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS Deliverable D7.3, 2005. http://www.fidis.net

Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum.* The role of data protection law and non-discrimination law in group profiling in the private sector", to be published in M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen*, forthcoming, Springer Press, 2007.

Scott, A. O., "A Future More Nasty, Because It's So Near", Film review of "Code 46", *The New York Times*, 6 Aug 2004.

Singsangob A., *Computer Software and Information Licensing in Emerging Markets, The Need for a Viable Legal Framework*, Aspen Publishers, 2003.

Sommer, Dieter, Architecture Version 0, PRIME Deliverable D14.2.a, 13 October 2004, pp. 35-6 and pp. 57-58. www.prime-project.eu.org

Sorkin, David E., "Technical and Legal Approaches to Unsolicited Electronic Mail", *University of San Francisco Law Review*, Vol. 35, 2001.

Spiekermann, S., and F. Pallas, "Technology Paternalism – Wider Implications of Ubiquitous Computing", *Poiesis & Praxis*, Vol. 4, no. 1, 2006.

Spiekermann, S., and M. Rothensee, *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing*, Institut für Wirtschaftsinformatik, Humbold-Universität zu Berlin, 2005. http://interval.hu-berlin.de/downloads/rfid/neuste%20forschungsergebnisse/SocioPsychofak.pdf.

Stajano, F., and R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", first *Security & Privacy supplement to IEEE Computer*, April 2002, pp. 22-26.

Stajano, F., and J. Crowcroft, "The Butt of the Iceberg: Hidden Security Problems of Ubiquitous Systems", in Basten et al. (eds.), *Ambient Intelligence: Impact on Embedded System Design*, Kluwer, Dordrecht, 2003.

Stout, David, "Data Theft at Nuclear Agency Went Unreported for 9 Months", *The New York Times*, 10 June 2006.

Streitz, N. A., and P. Nixon, "The Disappearing Computer", *Communications of the ACM*, Vol. 48, no. 3, 2005, pp. 32-35.

Sturcke, James, and agencies, "US access to flight data unlawful", *The Guardian*, 30 May 2006.

Subirana, B., and M. Bain, *Legal Programming: Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond*, Springer, New York, 2005.

Summers, Deborah, "Bureau admits innocents branded criminals", *The Herald* [Scotland], 22 May 2006.

Sutter Gavin, "'Don't Shoot the Messenger?' The UK and Online Intermediary Liability", *International Review of Law Computers & Technology*, Vol. 17 No.1, 2003, pp. 73-84.

SWAMI, "Safeguards in a World of Ambient Intelligence (SWAMI): Policy Options to Counteract Threats and Vulnerabilities – First Results", Report submitted to the participants of the SWAMI conference, Brussels, 21-22 March 2006. http://swami.jrc.es.

[US] Committee on Information Systems Trustworthiness, *Trust in Cyberspace*, National Research Council, National Academies Press, Washington, DC, 1999.

[US] National Telecommunications and Information Administration (NTIA), *Falling through the net: Towards Digital Inclusion. A Report on Americans' Access to Technology Tools*, U.S. Department of Commerce, Economics and Statistics Administration, National

Telecommunications and Information Administration, Washington, 2000. http://search.ntia.doc.gov/pdf/fttn00.pdf

Venkatesh, V., "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model", *Information Systems Research*, 11(4), 2000, pp. 342-365.

Vishwanath, A., "Manifestations of Interpersonal Trust in Online Interaction", *New Media and Society*, Vol. 6 (2), 2004, pp. 224 f.

Waelbroeck D., D. Slater and G. Even-Shoshan G [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004.
http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.html.

Weiser, M., and J. S. Brown, "The Coming Age of Calm Technology", in P. J. Denning and R. M. Metcalfe (eds.), *Beyond Calculation: The Next Fifty Years of Computing*, Copernicus, New York, 1997.

Welen, P., A. Wilson and P. Nixon, *Scenario Analysis*, Gloss Deliverable D.9, University of Strathclyde, Glasgow, 2003. http://iihm.imag.fr/projects/Gloss/Deliverables/D9-1.pdf.

Whitehouse, O., *GPRS Wireless Security: Not Ready for Prime Time*, Research report, @Stake, Inc., Boston, 2002.
http://www.atstake.com/research/reports/acrobat/atstake_gprs_security.pdf.

Wilkinson, L., "How to Build Scenarios", *Wired* 3, Special Issue. http://www.wired.com/wired/scenarios/build.html

Williams, Alun, "House of Lords to investigate Net security", PCPro, 28 July 2006.
http://www.pcpro.co.uk/news/91105/house-of-lords-to-investigate-net-security.html

Wright, David, "The dark side of ambient intelligence", *Info*, Vol 7 No. 6 [October 2005], pp 33-51. www.emeraldinsight.com/info

Wright, David, et al, "The illusion of security", *Communications of the ACM*, forthcoming [2007].

WWRF, *The Book of Visions 2001: Visions of the Wireless World*, Version 1.0, Wireless World Research Forum, 2001.
http://www.wireless-world-research.org/general_info/BoV2001-final.pdf.

Xenakis, C., and S. Kontopoulou, "Risk Assessment, Security & Trust: Cross Layer Issues", Special Interest Group 2, Wireless World Research Forum, 2006.

Zeller, Tom Jr, "For Victims, Repairing ID Theft Can Be Grueling", *The New York Times*, 1 Oct 2005.

Zinnbauer, D. et al, eInclusion Vision and Action: Translating vision into practice, vision paper, IPTS, Seville, 2006.

## 12.2 LEGAL TEXTS

Article 29 Data Protection Working Party, *Recommendation 3/97: Anonymity on the Internet* (WP 6), adopted on 3 December 1997, available through http://ec.europa.eu/justice_home/fsj/privacy/

Article 29 Data Protection Working Party, *Opinion on More Harmonised Information Provisions* (11987/04/EN - WP 100), adopted on 25 November 2004, available through http://ec.europa.eu/justice_home/fsj/privacy/

Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace* (5401/01/EN/Final - WP 55), adopted 29 May 2002, available through http://ec.europa.eu/justice_home/fsj/privacy/

Article 29 Data Protection Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites* (5035/01/EN/Final WP 56), 30 May 2002. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

Article 29 Data Protection Working Party in *Working Document on the Processing of Personal Data by means of Video Surveillance* (11750/02/EN - WP 67), adopted 25 November 2002, available through http://ec.europa.eu/justice_home/fsj/privacy/

Article 29 Data Protection Working Party, *Working document on biometrics* (12168/02/EN - WP 80), adopted on 1 August 2003, available through http://ec.europa.eu/justice_home/fsj/privacy/

Article 29 Data Protection Working Party, *Working document on data protection issues related to intellectual property rights* (WP 104), adopted on 18 January 2005. http://ec.europa.eu/justice_home/fsj/privacy/

Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology* (10107/05/EN - WP 105), 19 January 2005. Available through http://ec.europa.eu/justice_home/fsj/privacy/

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.

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, pp.29 –33.

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17/05/1991, pp. 0042-0046.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *Official Journal* L 095, 21/04/1993, pp. 29 – 34.

Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active medical devices, *Official Journal* L 323 , 26 November 1997.

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17/05/1991, pp. 0042 – 0046.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ* L 069, 16/03/2005 p. 67- 71.

Council of Europe - Cybercrime Convention of 23 November 2001.

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.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal* L 077, 27/03/1996, pp. 0020 – 0028.

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *Official Journal* L 144, 04/06/1997, pp. 0019 – 0027.

Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 On injunctions for the protection of consumers' interests, *Official Journal* L 166, 11/06/1998, pp. 51 – 55.

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 013, 19/01/2000, pp. 0012-002.

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, pp. 0001 – 0016.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal* L 167, 22/06/2001, pp. 0010 – 0019.

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), *OJ L* 108 , 24/04/2002 p. 0051 – 0077.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal* L 201, 31/07/2002, pp. 37- 47.

Green Paper on Conflicts of Jurisdiction and the Principle of *ne bis in idem* in Criminal Proceedings COM(2005) 696, December 2005, accesible at http://ec.europa.eu/comm/off/green/index_en.htm

Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations ("Rome II"), COM(2003) 427 final 2003/0168 (COD). http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0427en01.pdf

Tribunal de grande instance de Nanterre, 2 June 2004 (*UFC Que Choisir* v. *A O L Bertelsmann Online France*), available at http://www.legalis.net/jurisprudence-decision.php3?id_article=1211. For an English analysis, see Naylor, David, & Cyril Ritter, "B2C in Europe and Avoiding Contractual Liability: Why Businesses with European Operations Should Review their Customer Contracts Now", 15 September 2004. http://www.droit-technologie.org

**Deliverable Summary Sheet**

| | |
|---|---|
| Project Number: | IST-2004-006507 |
| Project Acronym: | SWAMI |
| Project title: | Safeguards in a World of Ambient Intelligence |
| Deliverable no.: | 4 |
| Due date: | July 2006 |
| Delivery date: | August 2006 |
| Delivery status: | Public |
| Work package no.: | 4 |
| Leading partner: | Trilateral Research and Consulting |
| Contributing partners: | All |
| Partners owing: | All |
| Distribution Type: | Public |