Information Society Technologies

SIXTH FRAMEWORK PROGRAMME

Safeguards in a World of Ambient Intelligence (SWAMI)

Deliverable D1

The brave new world of ambient intelligence: A state-of-the-art review

January 2006

Editors: Michael Friedewald, Elena Vildjiounaite, David Wright

Authors: David Wright, Elena Vildjiounaite, Ioannis Maghiros, Michael Friedewald, Michiel Verlinden, Petteri Alahuhta, Sabine Delaitre, Serge Gutwirth, Wim Schreurs, Yves Punie

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

If this report (or extracts from it) is used in the preparation of other reports, documents or publications, electronic or otherwise, the SWAMI consortium would appreciate acknowledgement of this report as a source. We suggest a citation like this: ”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“

Table of contents

1 Introduction

1.1 From ubiquitous computing to ambient intelligence

In 1991, Mark Weiser, chief scientist at the Xerox Palo Alto Research Center (PARC) in California, published a paper in *Scientific American* titled “The computer for the 21st Century” introducing his vision of a third generation of computing systems to a mass readership. Essentially, the vision described the historical transition from the large mainframe computers of the 1960s and 1970s to the standalone desktop personal computer (PC) of the 1980s and 1990s, and finally toward the networked computing appliance of the future. Third generation computing was presented as an integrated system of advanced computing devices, intelligent interface design, and anytime, anywhere data communications (Weiser 1991).

Weiser used the term *"ubiquitous computing”* to describe this third wave of computing systems, which marked the initial articulation of a vision of a future information society. What is most significant about Weiser’s vision is that while it pre-dated the mass diffusion of the Internet by a few years, it clearly embodies the idea of pervasive networked computers, assuming all kinds of shapes and located in all kinds of unconventional settings. Essential to the vision is networking, for without the ability of these computing devices to communicate with one another, the functionality of such a system would be extremely limited. In 1993, Weiser stated that the next generation computing environment would be one “in which each person is continually interacting with hundreds of nearby wirelessly connected computers” (Weiser 1993). At the time, such forms of wireless networking were still in their infancy, but today with wireless LAN, WiMax and Bluetooth, the possibilities for such dense local area networks are entering the realm of commercial reality.

While researchers in the United States were working on the vision of ubiquitous computing, the European Union began promoting a similar vision for its research and development agenda. The term adopted in Europe is *“ambient intelligence”* (coined by Emile Aarts of Philips) which has a lot in common with Weiser’s ubiquitous computing vision, while perhaps giving more emphasis to “human-centred computing” and to the vision as an integration or convergence of innovations in three key technologies: ubiquitous computing, user interface design and ubiquitous communication (for an overview, see Punie 2005).

In May 2000, the Information Society Technologies Advisory Group (ISTAG) commissioned the creation of four scenarios “to provide food for thought about longer-term developments in Information and Communication Technologies”, with the intent of exploring the social and technical implications of ambient intelligence. Among other things, the scenarios suggested a set of “critical socio-political factors” that were considered crucial for the development of ambient intelligence, including the issue of security and trust. ISTAG said that “a key aspect is management of privacy: more open systems tend to lower privacy levels [where] technological developments are outpacing regulatory adjustments” (ISTAG 2001). The scenarios developed for and assessed in the ISTAG report were regarded as a first step toward the creation of a research agenda in the EU that would contribute to the development of ”trust and confidence enabling tools” for the management of privacy within an ambient intelligence context. The ISTAG vision became a major focus of the “Disappearing Computers” component of the EC’s Fifth Framework Programme and provided a point of departure for structuring IST research under the Sixth Framework Programme of the European Union.

The Japanese have adopted the term *“ubiquitous network society”* to describe a vision that in many respects is being transformed into concrete action plans. They have put in place an initiative under the label “u-Japan Strategy” to replace the previous “e-Japan” policy framework (Murakami 2003). Similarly, a recently held policy roundtable titled “Realizing the Ubiquitous Network Society” addressed a range of issues that appear to be similar to those that underpin the EU’s ambient intelligence research programme. Results from the roundtable are intended as input to Japan’s emerging technology policy beyond 2006 and centre on a normative view that the country “must realize a ubiquitous network society in which convenient communications without restrictions will be allowed via broadband platforms, to which diversified equipment including [consumer equipment] will be connected.” The final report of this roundtable was published in late 2004 and has been posted on the website of Japan's Ministry of Internal Affairs and Communications (MPHPT 2004).

While IBM is credited with coining the term *“pervasive computing”* to refer to a shift in corporate computing systems, Philips chose the term ”ambient intelligence” to describe its new paradigm for home computing and entertainment. One of the first prototypes developed by Philips is a system that supports “smart home” applications based on collection and use of personal information that enables user preferences and creates user profiles for customising entertainment and other applications (Aarts/Marzano 2003).

Whereas companies like Philips are engaged in an ambitious vision that involves the private domain within the walls of the home, more mundane scenarios marking an important step toward the ubiquitous network society are being implemented today, often crossing into public space. One example is the growing use of RFID tags (radio frequency identification tags) to enable supply chain and inventory management in the private and public sectors (see e.g. Weis et al. 2004; Oertel et al. 2005). Representing an early entry point into pervasively networked environments, these tages contain radio-enabled microchips, attached to objects, which can be read out wirelessly. The growing use of RFID for supply chain management, access control and other applications indicates that the construction of the ambient intelligence (AmI) environment has already begun. However, the dramatic reduction in the cost of computing and communications and the rise of wireless broadband communications will facilitate the exchange of information among these early AmI devices and contribute to laying the foundations for the scenarios envisaged for the future. Above all, the networking of the proliferating devices in recent years demonstrates that the future, despite the still remaining formidable technological challenges, is not so far off.

While the technologists have been at work, goaded on by new and “old” high technology industries, concerns relating to identity, privacy, security, trust, social inclusion and other issues are beginning to get more airtime, too. The fears conjured up by the impact of an Orwellian Big Brother only complicate the apparent lack of trust, which hinders the full flowering of the Internet for e-commerce, e-government, e-health and much else. In November 2003, some 30 privacy advocacy groups joined together to produce a position paper calling for a halt to the deployment of radio frequency identification tags (RFIDs) until certain public policy issues are resolved (see for instance Albrecht 2002). Their concerns reflect a few of the more numerous and even more complex issues raised by ISTAG in its June 2002 position paper entitled “Trust, dependability, security and privacy for IST in FP6” (ISTAG 2002).

1.2 Challenges from the deployment of ambient intelligence

Ambient Intelligence should be seen as an emerging property (and not as a set of specific requirements) requiring a proper balance of a complex diversity of interests and values related to protection of identity, protection against intrusions by public and private actors, protection of the individual sphere (i.e., security), trust, protection against discrimination, access to information, free speech and so on. Such a balanced approach should take into account the different social, economic, legal and technological dimensions but also has to reflect many possible relevant perceptions and definitions of AmI. It also needs to embrace broader concerns such as, for example:

- the increasing concern for security after 11 September 2001;

- technological innovations, their dissemination and consequences, only some of which can be foreseen (the invisibility of networked “intelligent” devices, ubiquity of computer communications, anonymity and privacy impacts, user friendliness, price, accessibility, etc.);
- the general tendency toward privatisation of governance (the weakening of public power to control and steer the evolutions as a result of the increasing power of private actors both at local and global level).

Apart from the security concerns, AmI will directly affect our lives in many ways. Every one of us goes through life playing several different roles, which in essence could be reduced to three main ones – that of the private individual, the professional and the public participant.

Private individuals are mindful of their pursuits and/or responsibilities as parents or members of a family. They also have personal requirements in terms of entertainment, leisure and other activities such as shopping and may have special concerns in terms of health and/or education. According to the promoters of AmI, living in a world of ambient intelligence would greatly reduce the burdens (e.g. time) to pursue any of these things and greatly increase the richness of daily experience.

Similarly, the professional’s ability to communicate with his/her peers, either in the same office or on the other side of the world, to have an infinite world of information and intelligence at his/her fingertips to facilitate decision-making, will greatly expand with ambient intelligence.

In their public roles, citizens will participate in social and political activities, perhaps lobbying for or supporting this or that cause. In each of these roles, the citizen’s level of trust and confidence in supporting technology and in those with whom (s)he might be in contact will vary.

Citizens’ demands for privacy, security, trust (or confidentiality) will also vary according to the situation, and the situations may be very fluid, changing many times in the course of a day. In some of their roles, they will place demands on others; in others, they must place demands on themselves or accept certain responsibilities. In some roles and at some times, they will provide consent to others. At other times, they will seek consent (access) and at still other times, they may be unaware of the computing, monitoring and networking going on around them. At all times, they must be alert to the possibility of social engineering and threats to their space, to their digital well-being, if not their physical well-being. Individuals will need verifiable assurances that they can perform their various roles according to the level of privacy, security, trust, confidentiality and anonymity that they dictate. To understand the dimensions of this new world of ambient intelligence, to understand how it impacts them, what their rights and responsibilities are, how they can benefit from it, how they can control it, will be one of the objectives of our report.

Considering policy options and requirements in a world of ambient intelligence, research is needed, in particular addressing:

- issues such as privacy, anonymity, manipulation and control, intellectual property rights, human identity, discrimination and environmental concerns;
- new societal and policy options including responsibilities and ethics of digital behaviour;
- protection of rights for all citizens in all their roles (private and professional) in the Information Society;
- safeguards and privacy enhancing mechanisms to ensure user control, user acceptance and enforceability of policy in an accessible manner;
- equal rights and opportunities of accessibility to the Information Society and its ambient intelligence environment.

1.3 Challenges from ambient intelligence for EU policy-making

The definition of and provision for safeguards can be seen as critical for the rapid deployment and the further development of ambient intelligence in Europe. Moreover, they are in line with those of the IST priority and the broader Framework Programme 6 (FP6) objectives as well as related objectives stated by the Commission, the Council and others. The Framework Programme emphasises the importance of taking the human dimension into account in ambient intelligence. In doing so, it echoes the eEurope 2005 and the i2010 Action Plans that say that Europe should have a secure information infrastructure. To that end, they identify priorities for FP6 and FP7 as including trustworthy network and information infrastructures with an emphasis on emerging technologies like ambient intelligence. Research activities are expected to take into account the human factor in security (European Commission 2002, p. 16). The IST 2003 report puts it even more succinctly: Instead of making people adapt to technology, we have to design technologies for people (European Commission 2003b, p. 10).

Taking the human factor into account 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.[1]

Across the IST priority, special emphasis must be placed on, *inter alia*, measures to strengthen international co-operation. Such co-operation has already been initiated within the context of ambient intelligence, notably with the United States (European Commission 2003b, p. 117): Since 2000, the IST programme has developed strong relations with the US in this area, notably through the National Science Foundation and DARPA, the US defence research agency. As well as continuous dialogue at policy level, a series of joint events have been held and collaborations between the two RTD communities are being encouraged. It is therefore necessary to formulate options for the Commission and other policy-making bodies with further regard to international co-operation. In a networked world, best symbolised by the Internet, in which communications and computing capabilities know no borders, international co-operation is a must if the privacy and rights of individuals are to be protected. Many risks and vulnerabilities to Europeans emanate beyond our borders, hence social and policy options must include a global outlook. The Cybercrime Convention is an important step in this direction since its 34 signatories include more than just the Union’s Member States. In addition, representatives from the Commission, Member States and European industry participate in many standards-setting bodies concerned with cyber security and with a nominally global outlook. Nevertheless, more initiatives are needed in that direction. ISTAG also pointed out that it is important to take into account international co-operation in the quest for improved information and network security (ISTAG 2002, p. 10)

As Erkki Liikanen, former Commissioner for Enterprise and Information Society, stated in late 2003, FP5 provided important foundations for the vision of ambient intelligence, upon which the work in FP6 is being built (European Commission 2003b, p. 3). In the

[1] 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.

same report, it is stated that 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. Therefore it is high time to investigate whether the research policy of recent years has revealed lacunae with regard to policy development and if the scientific and industrial community has developed a hidden research agenda with priorities that are different from those considered important by public policy.

The definition of safeguards for the world of ambient intelligence is therefore relevant to the objectives and priorities of the EU's policy and regulatory framework, but its relevance in the wider world should also be apparent. For example, a recent roundtable of security experts identified the top ten security priorities for the next decade, with the first priority related to the "EverNet", which is, in effect, their way of labelling ambient intelligence. The experts' concern was summarised as follows: ”Billions of devices that are always on and always connected (…) increase the complexity of our systems to the point where it is not possible to comprehend all of what we are using (…) we need to resolve issues of identity and authority when these devices conduct activities for people without human intervention, when no one is around to notice” (Accenture / CERIAS 2001, p. 11). Thus, the experts were urging fast action to resolve these issues.

The definition of safeguards for a world of ambient intelligence will make important contributions to the scientific, technical, wider societal and policy objectives of IST policy on the European level. 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.

The new regulatory framework aims for a more secure environment for e-commerce transactions and to ensure an adequate level of consumer protection. Here it is necessary to examine the adequacy of the new regulatory framework in the context of the emerging technologies, capabilities and properties that are embedded in ambient intelligence. This can contribute to the strengthening of the three pillars (R&D, Regulation, Diffusion) upon which the European Union’s policy for the Information Society is based and, in particular, the second pillar which is the new regulatory framework covering all services or networks that transmit communications electronically (IST 2003b, p. 3).

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 a Report by the US Research Council on *Trust In Cyberspace* (Schneider 1999), 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 (see e.g. Thomas / Wyatt 1999). 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.

What is new in AmI is that devices with embedded intelligence are being networked and their numbers are set to increase by orders of magnitude. That has alarmed major privacy advocacy groups who, as briefly mentioned above, recently made a joint statement calling for a halt in the use of RFIDs until key issues are resolved. Meanwhile, companies such as Wal-Mart in the US, the Metro Group in Germany, Tesco in the UK and others are proceeding with their plans for a massive increase in the use of RFIDs, even before some standards issues have been resolved.

Similarly, location aware services have prompted concerns, even though they also offer many benefits. The increasing use of GPS in mobile phones in the United States in conjunction with services such as uLocate and Wherify Wireless enables those with mobile phones to be tracked wherever they go. While helping parents to know where their children are, the risks of unwanted and unwarranted surveillance have been highlighted by privacy advocates and others. Larry Smarr, director of the California Institute for Telecommunications and Information Technology, was quoted by *The New York Times*: "We are moving into a world where your location is going to be known at all times by some electronic device. (…) It's inevitable. So we should be talking about its consequences before it's too late." In the same article, it was asked whether federal investigators would be allowed to retrieve information on your recent whereabouts from a private service like uLocate or your cellular carrier. It also asks whether the local Starbucks store will be allowed to send advertisements to your phone when it knows you are nearby, without your explicit permission (Harmon 2003). These and similar examples highlight the need for urgent research in regard to the emerging world of ambient intelligence and, in particular, matters of privacy, security, trust, identity and so on.

The lack of consumer trust is often cited as the reason why e-commerce (and e-health and e-government) via the Internet is far from realising its potential. Attacks via the Internet are no longer confined to big name targets such as the military or credit card companies. Even individual users' home computers are being attacked or used as the staging platform for distributed denial of service attacks. Attacks are not only becoming more numerous, they are becoming much more sophisticated. The software security firm Symantec observed that, in July 2001, Code Red spread to 250,000 systems within six hours and the worldwide economic impact of the worm was estimated to be $2.62 billion. Code Red's spread was fast enough to foil immediate human intervention and the ramifications were huge. In the future, we may see the emergence of hypothesised threats that use advanced scanning techniques to infect all vulnerable servers on the Internet in a matter of minutes or even seconds (Schwarz 2003). Such reports and pronouncements undermine trust and confidence. SWAMI is looking not only at options aimed at increasing trust, but also at the steps that will take us toward what ISTAG has described as a new security paradigm.

Security must be regarded as an enabler for the development of new markets, not an inhibitor, which is a point stressed by the ISTAG reports on ambient intelligence. As an example of where security contributes to market development, one need look no further than the cars that we drive or the homes in which we live. Automobile manufacturers promote their products' various security features in marketing campaigns. Similarly, the insurance premiums we pay on our homes are diminished if we have installed security devices. In the electronic commerce area, some forms of business activities require or are facilitated by a particular level of trustworthiness (i.e., security is an enabler). As an example, the availability of secure socket layer (SSL) encryption for Web traffic has caused consumers to feel more comfortable about sending credit card numbers across the Internet.

Of particular relevance for the definition of safeguards is the ISTAG proposition that "Security policies in this [AmI] environment must evolve, adapting in accordance with our experiences. Such approaches may be very different from present approaches to computational security policies, but may better embody our approaches to real-world person-to-person trust policies. This is the main new feature of the new paradigm for security in AmI Space" (ISTAG 2002, p. 11). In the future AmI world, new approaches to security, trust, privacy, etc, will be required and it is urgent that such new approaches be considered before AmI becomes a reality, otherwise we, as a society, will be faced with a future akin to trying to squeeze toothpaste back into the tube. It will be difficult to embed retroactively new security and trust paradigms in AmI when those technologies have been deployed. The early definition of safeguards can contribute to the development of such new approaches.

The definition of AmI safeguards also contributes to the four lines around which the eEurope 2005 Action Plan was structured (European Commission 2002, p. 9ff.) which are, first, policy measures to review and adapt legislation at national and European level; second, implementation of policy measures supported by the development, analysis and dissemination of good practices; third, policy measures will be monitored and better focussed by benchmarking of the progress made in achieving the objectives and of the policies in support of the objectives; fourth, an overall co-ordination of existing policies will bring out synergies between proposed actions. In the recently announced i2010 action plan, the development of a strategy for a secure Information Society is a major part of the objective to create a single European Information Space offering affordable and secure high bandwidth communications, rich and diverse content and digital services:

> ”Trustworthy, secure and reliable ICT are crucial for a wide take up of converging digital services. During 2006 the Commission will propose a Strategy for a Secure Information Society to combine and update the instruments available, including raising awareness of the need for self-protection, vigilance and monitoring of threats, rapid and effective response to attacks and system failures. Support will be given to targeted research to ‘design-in’ security and to deployment measures that test solutions for key issues such as identity management. Revision of regulation will be considered where necessary, for example in protection of privacy, electronic signature or discouraging illegal and harmful content“ (European Commission 2005a, p. 6).

1.4 The objectives of the SWAMI project

The European Commission has recognised these challenges for European policy. It has stated that ”multidisciplinary research is needed on the social, legal, organisational and ethical issues 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“ (European Commission 2003a).

This project is addressing these issues by identifying and analysing possible “Safeguards in a World of Ambient Intelligence” (SWAMI). This includes 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.

SWAMI also intends to contribute to integrating and structuring the European Research Area mainly by generating awareness within the AmI community of the security, privacy, identity, accessibility and other issues that should be taken into account in the formulation and implementation of AmI projects, by providing the footing for related issues to be addressed in projects funded under the Seventh Framework Programme.

There is an urgent need for realising these objectives. Matters of identity, privacy, security, trust and so on need to be addressed in a multidisciplinary way in order for them to be enablers and not obstacles for realising ambient intelligence in Europe. Also, as often happens, the technology is progressing faster than the policy-building process that might otherwise assuage public concerns about the potential for new encroachments on privacy and engender trust in our technological future.

1.5 Objective and structure of the deliverable

The objective of the first SWAMI deliverable is to provide a state-of-the-art overview of the key social, legal, economic, technological and ethical implications with regard to identity, privacy and security of ambient intelligence as developed in existing scenario exercises, IST roadmaps and projects. For this purpose we have identified assumed functionalities available in scenarios and pinpointed the main technologies for producing these functionalities.

This deliverable comprises the results of the analysis of policy documents referring to the vision of ambient intelligence, the analysis of existing application scenarios developed as part of research and development projects and finally an investigation of the current legal framework in Europe with a view on its applicability for the emerging world of ambient intelligence. It identifies key social, legal, economic and other benefits of AmI as well as first evidence for possible threats.

Chapter 2 gives a selective overview of the various visions of ambient intelligence in the European Union, the United States and Japan. It is based on a review of the research that has been undertaken and the platforms, which have been created to realise these visions. A special focus is given to activities that already address questions of privacy, identity and security.

Chapter 3 presents the results of our analysis of existing scenarios for future AmI applications. After introducing the methodological framework, we give insight into the characteristics of typical scenarios that are used as the basis of R&D projects and present synthesised scenarios for the six most prominent application areas where AmI is expected to have a major impact. The analysed scenarios also indicate those enabling technologies playing a central role for the realisation of the AmI vision.[2] Finally we introduce those threats that researchers have already identified as being relevant for the acceptance of AmI applications and their deployment.

Chapter 4 gives an overview of the existing legal framework for ambient intelligence in the European Union. For each of the most important subject matters, it gives a description of the applicable law and identifies possible AmI-related problems and challenges in regard to privacy, identity and security.

[2] Note: While reference is given to main technologies, the focus of the deliverable is primarily on AmI applications and functionalities. It was not intended to give a comprehensive or detailed list of every technology, and certainly not a detailed technical description.

Chapter 5 summarises the main findings of our analysis and emphasis key challenges to be elaborated in greater detail in subsequent work packages.

2 AmI research in Europe, the United States and Japan

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 which provides a longer list of projects and their associated websites.

2.1 Introduction

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 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 somewhere a lot of personal information needs to be stored about the user. That being the case, there are 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 have also looked at various studies, reports and other documents.

We have 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.[3] 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 consider the platforms, i.e., the way in which industry, governments and other stakeholders have organised themselves to undertake the shared research agendas. We then draw the reader's attention to the key issues of privacy, identity, security, trust and the digital divide, point out safeguards that have been proposed and draw certain conclusions.

2.2 Ambient Intelligence in Europe

2.2.1 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).[4] *The Book of Visions* includes ambient intelligence within its scope. The first version of the *Book* appeared in 2001.[5] 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 (WWRF 2001, p. 39). In the envisaged security and privacy layer of future networks, customers should have the means to decide their security policies in a simple way.

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

[4] 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.

[5] www.wireless-world-research.org/general_info/BoV2001-final.pdf. The next version of *The Book of Visions* is to be published in spring 2006.

The Book says profile data have to be stored and managed in a user-acceptable way (perceived privacy is important). At the same time, this industry forum is of the view that "profile data-exchange and accessibility must not be restricted too much" in order to enable attractive and personalised mobile services (tailored to the user) (WWRF 2001, p. 128).

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" (WWRF 2001, p. 128).

Due to the nature of mobile services and use, profile data are gathered by multiple parties, stored in multiple places and used and managed by multiple stakeholders. The distributed nature of profiles must be supported by the architecture, says *The Book*. Further, both globalisation and virtualisation of society have contributed to a greater privacy risk. Protection of profile data and trust cannot be neglected in designing a service architecture for the next generation mobile setting. The user should have "optimal" [whatever that means] control over the use of his personal information (WWRF 2001, pp. 128f., 133).

While some of the statements in *The Book of Vision*s 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 Information Society Directorate General. In September 2003, ISTAG published a report called *Ambient Intelligence: from vision to reality* (ISTAG 2003).

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 (ISTAG 2003, p. 9).

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 (ISTAG 2003, pp. 11f.). The vision paper should be read in conjunction with at least two other ISTAG papers. One is on scenarios (see below), the other is on security and privacy issues.

2.2.2 Scenarios and application domains

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 (Welen et al. 2003, p. 6).

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 (ISTAG et al. 2001, p. 1).

Unlike other methods that explore the future with a single forecast (e.g., the Delphi method), scenario planning often involves generating several orthogonal futures using a matrix containing four quadrants with indicators as keys to the scenarios (Björk 2002).

There are different types of scenarios, as discussed in greater detail in a subsequent chapter of this report.[6]

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

[6] The ACIP project has three categories of scenarios, namely, descriptive versus normative scenarios; forecasting versus “backcasting” scenarios; common-sense-oriented, expert-based and constructor-based scenarios. Forecasting begins in the present and projects forward current trends to arrive at a possible future, while backcasting works from a possible future backwards towards the present. See O’Brien et al. 2003.

scenario “dark” are deficiencies with regard to privacy, security, identity and other issues of direct concern to SWAMI.

In this context, it is useful to consider the RAPID roadmap project (see below) 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.

The AMSD roadmap project (see below) is also of interest, because it analysed the ISTAG scenarios and others against dependability criteria, including privacy and security.

2.2.3 Roadmaps to the future

Roadmaps follow on from scenarios – i.e., to realise a scenario, roadmaps set out what steps must be taken. Roadmaps have become a strategic planning tool in many industries and even in international diplomacy (e.g., the US-brokered Middle East roadmap). 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 (Da Costa et al. 2003).

There are several European AmI-relevant roadmaps. One of the first was the PROGRESS **Embedded Systems Roadmap 2002**[7] 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.

Most of the roadmap is focused on embedded systems design, including general trends, user needs, technology requirements, system validation, etc. The roadmap also describes a new technology concept which it calls the Personal Well-being Assistant (PWA) which would fulfil user needs and embody technologies for different classes of users (youngsters, teenagers, young urban professionals, senior citizens). A major characteristic of the PWA is that its capabilities would be tailored for each individual user. It would be lightweight, portable or even small enough to be wearable. There might also exist a kind of base or docking station to interface with a local or global communication infrastructure. The individual user would be able to control or set the features he or she wants, including his or her personal privacy settings, which could vary depending on the context or time or type of transactions to be performed (Eggermont 2002, pp. 91f.).

Elsewhere, the roadmap makes the point that the growing needs for safety and security in electronic transactions and mobile communications leads to functionality extensions that must be designed-in.

Biometrics are likely to be an important technology in the AmI world of the future. The **BIOVISION** roadmap (June 2002-May 2003)[8] concerns future deployment of biometrics and, in particular, the secure, user-friendly, socially acceptable and ethical use of biometrics in Europe. The BIOVISION final report covers issues of identity and their implications for adoption of biometrics, applications, technologies and critical issues, including end user perceptions, security, safety, legal and regulatory dimensions, and standardisation. It investigated the commercial application of biometrics over the next 10 years using scenario modelling, noting the risks and potential benefits. It identified the research challenges and analysed existing R&D gaps.

[7] 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

[8] BIOVISION had a budget of €399,991 and nine partners. Its website is www.eubiometricforum.com

The **RAPID** project (July 2002-June 2003)[9] 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.

The **STORK** project (Aug 2002-Aug 2003)[10] developed a strategic roadmap for cryptology. It identified major European stakeholders in cryptologic research and applications, in both academia and industry, and the areas of existing or required research. It brought together key players in each area to formulate a common research agenda to meet current and future needs for cryptology. It identified topics for future research and laid the groundwork for a network of excellence in cryptology under the EC's Sixth Framework Programme.[11]

The **ACIP** project (June 2002-Apr 2003)[12] developed a roadmap for the analysis and assessment of Critical Infrastructure Protection (CIP). Critical infrastructures include banking and finance, energy, transportation, telecoms and others. Many AmI networks will form part of critical infrastructures, hence, issues such as security (not only network security but personal security) are important in critical infrastructure protection models. The vulnerability of critical infrastructures to attacks may result in unacceptable risks because of primary as well as cascading (secondary) effects. Costs and benefits of risk control are important considerations in achieving an adequate level of security.

The **AMSD** project (June 2002-August 2003)[13] was a dependability roadmap for the Information Society in general and embedded systems in particular. It investigated the various aspects of dependability (reliability, safety, security, survivability, privacy, etc.); education and training relating to dependability; and how best to encourage the

[9] 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.

[10] STORK is the acronym for Strategic Roadmap for Cryptology. The project had a budget of €200,000 and eight partners. Its website is www.stork.eu.org.

[11] The Network of Excellence is called ECRYPT. It was launched in February 2004. Its objective is to intensify the collaboration of European researchers in cryptology and digital watermarking. For more details, see the website: www.ecrypt.eu.org.

[12] ACIP is the acronym for Analysis & Assessment for Critical Infrastructure Protection. The project had a budget of €400,000 and 13 partners. The project's website is www.eu-acip.de.

[13] AMSD is the abbreviation for Accompanying Measure System Dependability. It had a budget of €399,979 and six partners. Its website is https://rami.jrc.it/roadmaps/amsd

widespread use by industry and governments throughout Europe of dependability best practice.

The **PAMPAS** roadmap (June 2002-May 2003)[14] is also of interest to SWAMI. That roadmap focused on ensuring that future mobile services and systems satisfy security, privacy and identity management requirements and produced a framework for future research. The project started from likely developments in mobile systems and applications, and identified their security and privacy requirements. Building upon this analysis, available technologies (e.g., cryptography, privacy-enhancing technologies, public key infrastructure, digital rights management) were investigated and mapped onto an application / technology matrix. In addition to open research aspects, the concluding assessment identified needs with respect to standardisation and regulation. The project developed a list of existing and emerging security and privacy-enhancing technologies. The PAMPAS roadmap also dealt with non-technical aspects (socio-cultural, economic, legal) and contains a SWOT-analysis from the European perspective.

The first edition of the **ITEA Technology Roadmap on Software-Intensive Systems** was released in March 2001.[15] The second edition was published three years later, in May 2004. The 267-page report mentions ambient intelligence 45 times, privacy 55 times, identity 68 times, and security 176 times. The ITEA Roadmap maps out five major application **domains**: home; cyber enterprise; nomadic; services & software creation; and intermediation services & infrastructures, all of which are relevant to AmI.

MEDEA+ is an industry-initiated, pan-European programme for advanced co-operative research and development in microelectronics.[16] The MEDEA+ **Applications Technology Roadmap** (ATRM) identifies a dozen challenges regarding the major technologies to be developed by 2012, two of which relate to

- security, safety and privacy issues penetrating into individuals' lives in both private and public domains;
- security, safety and privacy solutions that can be trusted, with new opportunities in digital rights management.

[14] PAMPAS is the acronym for Pioneering Advanced Mobile Privacy And Security. The project had a budget of €633,442 and seven partners. Its website is www.pampas.eu.org

[15] ITEA stands for Information Technology for European Advancement. Its website is www.itea-office.org. Like the MEDEA+ programme mentioned further on in this chapter, ITEA is a Eureka strategic cluster programme.

[16] www.medea.org

2.2.4 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:

The eMobility platform (see the section on platforms below) has also published a strategic research agenda. The latest version, available on its website,[17] is dated March 2005. A further revision is planned for September 2005. Major sections of its research agenda deal with ambient services, ambient connectivity, and security and trust.

The ARTEMIS platform (see next section) 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. The latest draft was set out at an ARTEMIS meeting in Paris in late June 2005.

2.2.5 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 (European Commission 2004b). 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 (European Commisson 2004a, 2005b). 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

[17] www.emobility.eu.org

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), both of which are mentioned below.

The following are platforms of interest to SWAMI:

Wireless World Research Forum (WWRF)

The Wireless World Research Forum (WWRF),[18] 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 might resolve the needs of users, operators, service providers and other players for secure and trustworthy wireless systems. SIG 2 plans to publish a White Paper in July 2005.

ARTEMIS

ARTEMIS[19] 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). In June 2005, ARTEMIS called for an increase of 40 per cent in funding ambient intelligence research by 2010.[20]

[18] www.wireless-world-research.org

[19] 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/

[20] http://ica.cordis.lu/search/?fuseaction=news.simpledocument&N_RCN=24083

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[21] 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.

2.2.6 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 issues in a substantive way. None of the AmI projects specifically addresses the digital divide issue, although the PROFIT project warns of an “ambient divide” between those who accept the benefits of AmI and those who fear a loss of control over personal data. 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). PISA inspired follow-on projects, notably PRIME, but also the Dutch PAW project. The privacy projects mainly focused on privacy enhancing technologies and identity management in the context of legal requirements. Or, to put it differently, the projects focused more on technological solutions to the threats to privacy, identity and security, and less on non-technological solutions, i.e., those of a policy, regulatory, economic or social nature (which is what SWAMI aims to do).[22] Interestingly, a third of the privacy

[21] www.emobility.eu.org

[22] The PAMPAS and RAPID roadmaps were an exception; they dealt with non-technical aspects (socio-cultural, economic, legal). PISA and PRIME also dealt with legal requirements.

and identity projects were roadmaps, but all of those had or have budgets of somewhat less than €1 million.

Some of the privacy projects were reviewed by Marc Langheinrich from the Swiss Federal Institute of Technology in Zurich (ETHZ) who prepared a short paper as a Disappearing Computer (DC) initiative called Troubadour. His conclusion was that, even though general concerns for privacy remain high, few researchers have actually thought about such problems in depth (Langheinrich 2003).[23]

While Langheinrich may have a point, nevertheless there have been a reasonable number of projects specifically focused on privacy, identity, etc. and still others which have dealt with such issues in a substantive way in the context of more encompassing research objectives. Some of these are mentioned in the section on roadmaps. Among the various projects which have considered privacy, identity, security, trust and digital divide issues are PISA, PRIME, GUIDE, FIDIS, BASIS, PAW, EUCLID, eEPOCH, AMBIENT AGORAS, GROCER, AMSD, OZONE and BITE, which are further referenced below.

Given the expected pervasiveness of ambient intelligence in the years to come, the growing problem of identity theft, and concerns about digital divides, clearly AmI projects need to take into account privacy, security, identity and related issues. To the extent that security has been considered, it has mainly been an issue of network security rather than individual security.

2.2.7 Privacy

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-

[23] www.vs.inf.ethz.ch/res/papers/dctales-privacy.pdf. See also UbiSoc 2005: Workshop on Social Implications of Ubiquitous Computing. http://www.chi2005.org

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

As noted above, several European projects have focussed on privacy issues and have articulated certain principles and proposed various safeguards. Among them are the following:

The **RAPID** project, mentioned earlier, developed a strategic roadmap for applied research in the area of privacy and identity management.

The **PISA** project (Jan 2001-Jan 2004)[24] focused on development of new privacy enhancing technologies (PETs) for electronic business and demonstration of PETs as a secure technical solution to protect the privacy of individuals when they use intelligent agents.

The **PRIME** project (Mar 2004-Feb 2008)[25] is a follow-on to PISA. PRIME aims to develop solutions for privacy-enhancing identity management for end users. The PRIME consortium expects to help citizens manage their privacy and to support business in its compliance with privacy data processing requirements.

The Dutch **PAW** project (Oct 2003-Oct 2007)[26] is developing a privacy protecting architecture to protect the user's privacy in an ambient world. The project takes a two-tier approach. To prevent unwanted collection of data about a user and his actions, techniques from secure computing are extended to provide private computing. To control the authorised dissemination of data about a user, licensing techniques similar

[24] PISA is the acronym for Privacy Incorporated Software Agent. The project had a budget of €3.2 million and nine partners. Its website is www.pet-pisa.nl/pisa_org/pisa/index.html.

[25] PRIME is the acronym for Privacy and Identity Management for Europe. The project has a budget of €13.14 million and 21 partners. Its website is www.prime-project.eu.org

[26] PAW is the acronym for Privacy in an Ambient World. The project is funded by the Dutch Ministry of Economic Affairs through the IOP GenCom programme managed by Senter. PAW is additionally supported by funds from TNO Telecom. It has four partners. Its website is www.cs.ru.nl/~jhh/paw/index2.html

to those used in digital rights management are being considered. Inter alia, the PAW project proposal says that privacy protection can be divided into several categories:

1. Protecting a person's identity

2. Protecting an identity's personal data

3. Protecting the actions of an identity

4. Protecting the instructions or tasks of an identity

To provide full privacy, adequate solutions must be found for each of these categories.

2.2.8 Identity

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.

The concept of identity can be approached from a number of standpoints, as the BIOVISION project has noted: for example, we can view it from philosophical, psychological, sociological, legal and technical perspectives, which suggest that there is a risk that identity management systems could be over-bearing in their complexity or requirements imposed on the individual. Of even more concern are possible unforeseen long term consequences of fixing identities, and the impact of such fixedness if identities are reused in different domains ('function creep') (Rejman-Green 2003, p. 14), as is the case when a driver's licence is used to establish identity.

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 any e-government service, but so far no standard authentication system is accepted and widely used by citizens. The GUIDE project (Jan 2004-June 2005),[27] 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

[27] 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

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),[28] 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
- 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. For example, in Germany an ID card is mandatory for every adult, while in the UK state-issued ID cards do not exist (yet). FIDIS aims to help shape the requirements for the future management of identity in the European Information Society and contribute to the technologies and infrastructures needed.

[28] 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

Although the EUCLID project (Apr 2002-Nov 2003)[29] was not an AmI project, nevertheless it is relevant to the search for safeguard. EUCLID promoted a common approach to the implementation of digital ID in Europe. In this, it was helped by the 65-page Electronic Identity White Paper[30] which provided an overview of efforts across Europe regarding deployment, functionality and technologies needed to harmonise the usage of electronic smart cards.

The eEPOCH project (Nov 2002-Oct 2004)[31] had a somewhat similar focus. It aimed to demonstrate the technical specifications formulated by the eEurope Smart Card Charter to guarantee the interoperability of smart cards in terms of European citizens' identification, authentication and signature. It looked at secure, smart-card-based, digital identification systems providing the levels of trust and confidence necessary for citizens to interact digitally with their national and local administrations and other European institutions. It aimed to enable cross-border electronic signature for legal purposes, offer reliable identification based on data in government databases, and ensure secure authentication of the cardholder and device on the basis of PINs, biometrics and PKI (Public Key Infrastructure) mutual authentication.

eEPOCH also produced an 18-page "White Paper" (not to be confused with the aforementioned Electronic Identity White Paper) entitled *e-ID and the Information Society in Europe* (ePOCH 2003). Electronic identity (e-ID) allows a person or legal entity to be recognised and authenticated online. The White Paper says online communication and transactions necessitate efficient, unambiguous, widely accepted identity. Theoretically, this identity could be based on a code or digitised biometrics. This presupposes the deployment of a central database containing all data associated with each set of codes or biometrics which can check the identity data stored on a "token" incorporating a microchip. The most common token today is the smart card. For online use, says eEPOCH, it is not efficient to make completely different tokens for the same function in different environments. Applying standards for the cards, the data and the card-issuing procedures makes more sense than creating and maintaining different e-IDs for different applications that use more or less the same e-ID data.

[29] EUCLID is the acronym for European initiative for a Citizen digital ID solution. The project had a budget of €674,337 and four partners. Its website is www.electronic-identity.org.

[30] www.electronic-identity.org/experts.shtml. This is version 1.0 dated June 2003.

[31] The full title of the eEpoch project is eEurope Smart Card Charter proof of concept and holistic solution. The project had a budget of €4.97 million and 16 partners. Its website is www.eepoch.net

2.2.9 Trust

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

The issue of trust is mentioned in various projects, usually in an incidental way. The issue gets attention in the context of building trustworthy capabilities that can still serve their purpose on untrustworthy networks. However, no project specifically focuses on trust from the point of the individual AmI user or even more specifically 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. This is somewhat surprising in the sense that some level of trust must exist before the user is willing to try out a new technology. Clearly, system and network designers should (must) build security in all parts of the architecture as a first step towards earning the user's trust. They must also satisfy the increasingly aware user that her privacy will be respected (and that there are remedies if it is not) and the risk of identity theft can be diminished. Only then can they hope to gain her trust – and even then, she may not put her trust on the line because her perceptions have been influenced by, for example, the many stories she has read in the online newspapers about security flaws. 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.

2.2.10 Security

As noted earlier, ISTAG has said that AmI will require security solutions very different from those of today's systems. It postulates 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. The ISTAG vision is somewhat congruent with that in WWRF's *Book of Visions* which said (as also noted earlier) that customers should have the means to decide their security policies in a simple way.

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 is an important issue for network operators, service providers and citizens, and it comes therefore as no surprise that various European projects have focused on security issues. The AMSD project (June 2002-Aug 2003)[32] considered these issues: (i) information infrastructure interdependencies and vulnerabilities, (ii) privacy and identity management, (iii) trust and security in e-business processes, and (iv) dependable embedded systems. It re-examined the ISTAG scenarios in the context of potential threats to privacy, trust, user confidence and dependability.

Like others, the OZONE project (Nov 2001-Aug 2004)[33] recognised that security and privacy are prerequisites for consumer acceptance of new ambient intelligence systems and, accordingly, took these into account in the project's software environment objectives.

eMobility says security is essential in all parts of the future network architecture and that the challenge for the future security framework is to maintain simplicity and efficiency. The level of offered security should adapt the service needs in terms of user authentication, information encryption, privacy, anonymity, identity management, and content delivery. It notes that security threats may have implications for the regulatory framework and that research effort and results should be taken into account when reviewing the regulatory framework for electronic communication in 2006. It also says user needs should be taken into account in any research while user trials should capture the user perspective on security.

The eMobility research agenda appears to be sensitive to privacy and security consideration. It says, for example, that future service platforms must address new security requirements, among which it identifies:

- Trusted platforms for mobile security & privacy
- Mobile application security & privacy
- Privacy-preserving mobile applications with tuneable anonymity
- Location-based services versus location privacy
- Secure transactions (especially mobile payments)
- Secure content handling (DRM)

[32] AMSD is the abbreviation for Accompanying Measure System Dependability. It had a budget of €399,979 and six partners. Its website is https://rami.jrc.it/roadmaps/amsd

[33] The full title of the OZONE project is New technologies and services for emerging nomadic societies. The project had a budget of €12.21 million and nine partners. Its website is http://www.extra.research.philips.com/euprojects/ozone/. See also www.hitech-projects.com/euprojects/ozone/

- Secure interoperability between services offered to different environments (multi-technology and multi-operator covering both wireless and fixed access)
- User-centric mechanisms allowing (authorising) controlled release of personal information
- Secure user identity management
- Single sign-on based on mobile authentication
- Authorisation privacy
- Authentication via security tokens using mobile devices
- Defence and response to security attacks

2.2.11 Digital divide

Apart from the ISTAG scenarios, the digital divide issue has scarcely figured in any AmI projects, except in the sense that there is widespread agreement that AmI technology should be either invisible or easy to use. One of the few projects to consider the digital divide issue was PROFIT (June 2003-June 2004), which was sponsored by Eurescom, a Heidelberg, Germany-based association of telecom operators (such as BT, Deutsche Telecom, France Telecom, etc).[34] The project investigated socio-economic and business issues related to AmI, including the relationships between people's social identities and the adoption of ICT services. PROFIT interviewed real users in UK, Finland, Norway and Hungary to find out wishes, unmet requirements, concerns and barriers related to AmI services. The project found that people preferred to have an identity verification device which only offered an extremely "hollowed out" form of identity verification, confirming who they say they are with simple biometric data. Respondents were concerned that in the AmI world they would lose control over how their personal information was used. Other respondents felt that being surrounded by AmI devices would lead to a loss of independence or an over-reliance on technology which could cause "tremendous" problems if there were systems failures and even a de-skilling in how to do things. PROFIT concluded that the ambient intelligence divide is likely to be greater than the digital divide for a number of reasons including poor user perceptions, lack of willingness to pay for devices or services which already exist in

[34] PROFIT is the acronym for Potential pRofit Opportunities in the Future ambient InTelligence world. The project deliverables can be obtained after registration at the website. See www.eurescom.de/public/projects/P1300-series/p1302/P1302_portal.asp#P1302%20Deliverable%201

another form and are available free or cheaply, and the reliance on technological prerequisites, such as using an electronic diary (Ellis 2004, p. 8).

User trials and surveys, such as those conducted by OZONE, PROFIT, AMIGO, EQUATOR and others, are a good idea to test the responsiveness of users to new security, privacy and related solutions.

2.2.12 Safeguards

From our review of more than 70 European projects, the principal types of safeguards have centred on the following:

Privacy enhancing technologies (PETs)

PETs involve fundamental technologies and include the human-computer interface, ontologies, authorisation and cryptology. An example of a PET is the Personal Well-being Assistant envisaged by the Embedded Systems Roadmap. The individual user would be able to control or set the features he or she wants, including his or her personal privacy settings, which could vary depending on the context or time or type of transactions to be performed (Eggermont 2002, pp. 91f.). Conceptually, the notion of a PWA as an interface with the ambient intelligence environment with “tuneable” privacy and security levels is interesting for SWAMI as a potential safeguard. Even better, the PWA as envisaged by the roadmap would be able to advise users, e.g., if they weren’t sure what level of privacy protection would be appropriate in a particular context.

The eMobility platform has identified other technologies to be exploited in order to build a reliable security framework including wireless PKI, XML security, SIP security, firewall technologies, etc (Tafazolli et al. 2005, p. 32-33).

Biometrics

The use of biometrics has been the focus of several projects. Biometrics use physical or behavioural information to identify a person. The data used can range from fingerprints, to iris scans, to DNA. Application of the technology involves comparing the information obtained from someone on the spot with that stored in a databank in order to verify identity. While biometrics may be a useful means of authentication, they also raise concerns about the security of the stored data against which biometric matches are made. Also biometrics may not be feasible in some instances, for example, due to some physical disability (blindness, absence of a hand, etc). Like many other technologies, biometrics could be subject to abuse and may work to the detriment of privacy and identity protection (Maghiros et al. 2005). While DNA and genetics have already been used as identifiers in forensics, new problems may arise if they are used more generally. Ethical issues involving biometrics are the subject of the FP6-funded project BITE ("biometric identification technology ethics"), which began in Oct 2004.[35]

There is no shortage of advocates of biometrics, but the BIOVISION project determined that the key factors governing deployment of biometrics are user concerns (notably privacy), security of devices and systems, legal and regulatory issues, and standardisation. BIOVISION emphasised that biometric technologies should be viewed as mechanisms that address one aspect of an application. Whether the use of biometrics enhances or reduces personal privacy, improves or worsens security, makes authentication more or less convenient will depend on other features of the application (Rejman-Greene 2003, p. 6). With a view to societal concerns about biometrics, the BIOVISION consortium developed a deliverable on best practices on privacy and security issues.

The Dutch BASIS project (Dec 2003-Nov 2007)[36] is also investigating the possibilities of biometric authentication for securing access to information and services. The project is addressing several problem issues related to transparent biometric authentication (i.e., not requiring specific user actions) as a means to enhance user convenience; anonymous biometric authentication (i.e., not requiring the storage of privacy-sensitive biometric data) as a means to protect the user's privacy; and the use of biometric authentication in the home environment (Beumer et al. 2004).

Cryptography

Encryption has been a way of protecting communications and storage of personal data for many years, and inevitably will continue to be an important means of safeguarding privacy and identity and increasing security and trust in the AmI world as well. By itself, cryptography is not sufficient to ensure the requirements, but still it will be part of the solution. Thus, the work undertaken by the STORK project and its follow-on ENCRYPT network of excellence needs to be taken into account in prospective safeguards.

Intelligent software agents (ISA)

An intelligent software agent is software and/or hardware acting in order to accomplish a task on behalf of its user, like a servant, but with minimal intervention by the user. A

[35] The BITE website is www.biteproject.org.

[36] The project has funding of €740,000, coming from the IOP Generic Communications (GenCom) programme of the SenterNovem Agency, the Dutch agency for sustainable innovation. The project has three partners. Its website is www.sas.el.utwente.nl/home/basis. See also Beumer et al. 2004.

software agent could run on a user's computer but could also move around on the Internet or other networks. While executing its task, an agent can collect, process, store and distribute data. Some of these data could be about individuals and might be privacy-sensitive or become privacy-sensitive when the agent processes personal data or combines them with other data. The PISA project developed an ISA model to protect users' privacy in a networked environment. The PISA project showed how PETs could perform complex actions without personal data being compromised.

Software agents such as those considered by the PISA and PRIME projects appear to be promising technological developments for enhancing privacy and security. Of course, one cannot be reliant on a single solution. A layered approach to security is better.

Legal and regulatory safeguards

Legal and regulatory measures to protect privacy and to prosecute those engaged in identity theft have been considered by several projects. The PISA project produced a 372-page handbook entitled *Privacy and PET*. The handbook shows which privacy law rules apply to ISAs and how to implement a privacy-incorporated software agent (PISA). The handbook covers the handling of personal information and plans for organisations to carry out a privacy audit of their data protection measures. The PISA project considered new threats to data security in environments using software agents, as well the challenges of evaluating compliance with data protection standards, assessing privacy protection before implementation in systems that use thousands of software agents, and building human-computer interfaces promoting trust in system security.

GROCER (Feb 2001-Jan 2004)[37] was another project that considered legal and trust issues including privacy and consumer protection risks and requirements, software agent-based transactions and legal engineering, i.e., building compliance into ICT architectures.

Licensing

One novel approach to privacy protection is that being considered by the Dutch PAW project. To control the authorised dissemination of data about a user, licensing techniques similar to those used in digital rights management are being considered. In particular, a private licensing language and protocols to handle and enforce such

[37] GROCER is the acronym for Grocery Store Commerce Electronic Resource. It had a budget of €2.23 million and three partners. Its website is www.cordis.lu/ist/fet/dc-sy.htm.

licences is being developed. Ambient systems are characterised by their low resources and capabilities. PAW's key challenge is to develop an efficient architecture to implement its ideas.

Procedural safeguards

Taking note of a comment by Bruce Schneier ("If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."), procedural safeguards should be on the list. Procedural safeguards include actions such as privacy audits as well as physical security.[38] The ISO standard 17799:2005, which provides a code of practice for information security management, is a prime reference source for implementing procedural safeguards.

Guidelines

Not all measures need to be legal or regulatory in nature. Voluntary compliance with industry guidelines also have a role to play in protecting privacy. The AMBIENT AGORAS project (Jan 2001-Dec 2003)[39] recognised that some users could fear the increased possibilities of being observed and of losing control over private information due to the hidden functionality of invisible embedded devices. Since the use of sensing technology for the detection of people raises privacy concerns, the project developed Privacy Design Guidelines for systems designers (Lahlou/Jegou 2003; Langheinrich 2001).

The guidelines make the point that privacy enhancement is better obtained by actively constructing a system exactly tailored to specific goals than by trying to defend ex-post a poor design against misuse or attacks. The nine guidelines are as follows:

1. *Think before doing*

Evaluate potential system impacts. The very nature of a system or its parts may be against privacy in their intention.

2. *Re-visit classic solutions*

[38] *The New York Times* recently reported an incident where personal data transported in a van went missing (Stross 2005)

[39] The full title of the Ambient Agoras project is Dynamic Information Clouds in a Hybrid World. The project had a budget of €3.28 million and four partners. Its website is www.ambient-agoras.org

Search for existing solutions in the physical world or in old systems for the similar class of problem/service, and understand the way in which new technologies change the effects of classic issues.

3. *Openness*

Systems should give user access to what they do, do it, and do nothing else. Help subjects [=human users] construct a valid and simple mental model of what the system does. Goals, ownership and state of system should be explicit, true, and easily accessible to subjects, in a simple format.

4. *Privacy razor*

Subject characteristics seen by the system should contain ONLY elements which are necessary for the explicit goal of the activity performed with the system. No data should be copied without necessity. In case of doubt, remember further information may be added in context.

5. *Third party guarantee*

Using a neutral or trusted third party may open more solutions or lighter design. It may enable entitlement, validation, control, claim, archive, etc. without direct data transfer between system and subject. In case of third party involvement, give the user choice.

6. *Make risky operations expensive*

No system is 100 per cent privacy safe. Subjects should be made aware of which operations are privacy-sensitive. Operations identified as privacy-sensitive should be made costly for the system, the subject, the third party. In some cases, this guideline can be dangerous (e.g. access to medical data in emergency situations).

7. *Avoid surprise*

Subjects should be made aware when their activity has an effect on the system. Acknowledgement should be explicit for irreversible major changes. Cancellation should be an option as much as possible, not only in the interface, but in the whole interaction with the system.

8. *Consider time*

Expiry date should be the default option for all data.

9. *Good privacy is not enough*

Safety, security, sustainability, equity… are important issues with which trade-offs may have to be considered. These trade-offs should be discussed with stake-holders or their representatives as much as possible.

Older and still relevant guidelines have been produced by the OECD, notably its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980. Its more recent Guidelines for the Security of Information Systems and Networks is an equally important reference.

2.3 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 team have 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. Security from both of these perspectives has featured in US projects and studies (see also Maghiros 2003).

The importance of security as a subject of research in ubiquitous computing can be neatly summarised from a statement made by a computer scientist from the University of California at Berkeley before a Congressional committee. He spoke partly in support of the TRUST proposal which he and his colleagues had put together, but his remarks had wider relevance to the security issue. He said:

> ” The last decade has seen a rapid increase in computer security attacks at all levels, as more individuals connect to common networks and as motivations and means to conduct sophisticated attacks increase. In today’s environment there is heightened awareness of the threat of well-funded professional cyber hackers and the potential for nation-state sponsored cyber warfare. Cyber attacks are increasingly motivated by the financial gain and global politics. A parallel and accelerating trend of the last decade has been the rapidly growing

> integration role of computing and communication in critical infrastructure systems, such as financial, energy distribution, telecommunication and transportation, which now have complex interdependencies rooted in information technologies“ (Shastry 2003).[40]

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),[41] which is the central research and development organisation for the Department of Defense (DoD).

Probably the next most important source of funding is the National Science Foundation (NSF)[42], which has been funding cyber security research through various of its programmes, notably those under the responsibility of the NSF’s Directorate of Computer and Information Science and Engineering (CISE). The NSF is an independent federal agency with an annual budget of about $5.5 billion, funding about 20 per cent of all federally supported basic research in US colleges and universities.

The Department of Homeland Security (DHS) through its Science and Technology Directorate is growing in importance as a source of funding for cyber security research.[43]

Government agencies such as the Energy and Transportation departments have been funding ubiquitous computing research as well. The Transportation Department has, for example, funded studies to put sensors on cars and trucks to help them avoid collision. The department also is exploring the idea of embedding roads, bridges and runways

[40] A perhaps countervailing view has been put forward by security expert Bruce Schneier at an Infosecurity Europe conference in London in April 2005. Schneier claimed that cyberterrorism was a myth, promoted by security companies looking to boost their sales. "Nobody's getting blown to bits," said Schneier. "I don't think that cyberterrorism exists — if you add 'terrorism' to things, you get more budget. If you can't get email for a day, you're not terrorised, you're inconvenienced." Schneier added: "We should save 'terror' for the things that deserve it, not things that piss us off." Quoted in Waerden 2005.

[41] www.darpa.mil

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

[43] 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).

with networks of sensors that could broadcast information about driving or aircraft landing conditions under a program called Intelligent Transportation Systems (quoted in Ricadela 2005).

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.[44]

2.3.1 Visions

We have not come across (at least, not yet) any outstanding vision document, like *The Book of Visions*, relating to ubiquitous computing. This does not mean, of course, that there are not visions of the brave new world. On the contrary. It’s been said that the *Embedded Everywhere* report published by the National Academy of Sciences (NAS) is such a vision document, but in fact it is explicitly a research agenda (NRC/NAS 2001). 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.[45]

Information technology is increasingly all around us. Often we are not aware of its presence, but it has led and is leading to a significant erosion of our privacy, even as it touts the benefits of enhanced security. The authors of the *Embedded Everywhere* report saw this happening too (“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

[44] 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).

[45] 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 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

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.

2.3.2 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 (to continue to take that report as an example), 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 (Garlan et al. 2002). Another is the Portolano project which comes not only with a "screenplay" and analysis, but even with cartoons.[46]

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 (Kent/Millett 2003, pp. 21-27). 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.

2.3.3 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

The best known roadmap, at least in the world of semiconductors, is the International Technology Roadmap for Semiconductors (ITRS),[47] which is an assessment of the technological challenges and needs facing the semiconductor industry 15 years into

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

[47] http://public.itrs.net/

the future and potential solutions. The objective of the ITRS is to ensure advancements in the performance of integrated circuits. This assessment is a co-operative effort of the global industry manufacturers and suppliers, government organisations, consortia, and universities. The most recent full revision of the roadmap occurred in 2001. Updates and revisions to the ITRS have been made annually since then.

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. Its utility to the SWAMI project is therefore negligible.

2.3.4 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). Also, work has been proceeding since about 2000 on yet another report to be entitled *Privacy in the Information Age*. It is due to be published towards the end of 2005. A 10-page abstract of this latter report is available on the CSTB website. Another report in the works is *Whither Biometrics?* It is expected to be published in 2006.[48]

Embedded Everywhere

DARPA and the National Institute of Standards and Technology (NIST) asked the National Research Council (NRC) to conduct a study of networked systems of embedded computers. The objective was to develop a research agenda that could guide federal programmes related to computing research and inform the research community (in industry, universities and government) about the challenging needs of this emerging research area (NRC/NAS 2001).

Although the 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".

[48] http://www7.nationalacademies.org/cstb/project_privacy_prospectus.html.

The following points have been extracted from the report.

EmNets are capable of collecting, processing, and aggregating huge amounts of data. With the advent of large numbers of EmNets, the technological stage is set for unprecedented levels of real-time human monitoring. The sensors are cheap and unobtrusive, the computing and communications costs are very low, and there will be organizations with the resources and the motivation to deploy these systems. Thus, EmNets present a difficult challenge in terms of passive information disclosure … In the case of EmNets, inadvertent, even unintentional revelations are much more likely. (NRC/NAS 2001, pp. 181f.).

In many cases, individuals may be unaware of sensor networks deployed in the public spaces or commercial environments they enter and the associated information being collected about them. Even in their own homes, many users may be unaware of the types of information that embedded processors are collecting and possibly transmitting via networks to vendors or other recipients.[49] The embedding of information technology into a growing number of devices will increase the amount of personal and personally identifiable information that can be collected, stored, and processed.

A related 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 (NRC/NAS 2001pp. 135f.).

The 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 (NRC/NAS 2001, p. 137).

The *Embedded Everywhere* report raised many security and privacy related questions and issues which are similar to those raised by ISTAG (2002). Many of the questions and issues remain to be resolved.

[49] *Embedded Everywhere* has a footnote at page 134 giving an example: Few automobile drivers, for example, are currently aware that many cars collect and store information about the way a car has been driven (e.g., driving speed, acceleration, engine speed). This information can be used by manufacturers to better analyse accidents and, hence, improve safety but could also be used to disallow warranty claims or to prove that an automobile was operated in an unsafe manner.

Who goes there?

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

4. *Communications privacy*, a subset of information privacy that protects the confidentiality of individuals' communications (Kent/Millett 2003, p. 63).

The report identifies four overarching privacy concerns that broadly characterise the risks to personal privacy that authentication systems can create (Kent/Millett 2003, pp. 30f.):

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.

RFID workshop

As a follow-on to *Embedded Everywhere,* the National Research Council conducted a workshop that explored RFID technology and related technical and policy issues (NRC 2005). Workshop participants included representatives from industry, academia, government and non-governmental organisations. The following points were made during the workshop:

Tags on or near individuals can be read without their knowledge, the tags can potentially be on everything in an individual's possession, and individuals could carry a complex, unique constellation of data (that is, of the full set of IDs on an individual's person or in his or her possession). RFID systems enable at least a scaling up, if not a change in the nature of surveillance and in the character of information collection that is possible (NRC 2005, p. 23).

Risks and benefits must be explored before the technology is fixed—that is, before the technology has been fully designed and developed for its various, specific applications. There is likely to be tremendous benefit in a design approach that precedes any sort of legislative or regulatory solution, not only because the resultant technology will almost certainly be more elegant, but, more importantly, because the public trust would not have been undermined. Should cultural concerns (privacy, security, legality, equity, and so on) be inadequately accommodated, a backlash of some sort is more likely to occur. Moreover, if lack of attention to privacy and social concerns means that advocates are forced to be more confrontational in order to have their concerns heard, it is possible that socially constructive uses of RFID technologies, from education and medicine to commercial applications, will be stymied (NRC 2005, p. 25).

2.3.5 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.

The apparent scarcity of platforms in the European sense troubled the authors of the *Embedded Everywhere* report. They said that some of the questions raised in their report would be best addressed through a concerted effort. Leaving this work solely to the private sector, they said, raises a number of troubling possibilities. Of great concern is that individual commercial incentives will fail to bring about work on problems that have a larger scope and that are subject to externalities: inter-operability, safety, upgradability, and so on. Moreover, a lack of government funding will slow down the sharing of the research, since the commercial concerns doing the research tend to keep the research private to retain their competitive advantage. The creation of an open research community within which results and progress are shared is vital to making significant progress in this arena (NRC/NAS 2001, p. 9).

The authors added that ensuring that the right kinds of research are conducted to advance the state of the art in EmNets will require changes in the way the nation's research enterprise is organised. Effective collaboration will be needed not only among industry, universities, and government, but also between IT researchers and researchers in other areas that will make use of EmNets (e.g., the health sciences, manufacturing, and defence). Explicit efforts will need to be made to put mechanisms in place for ensuring such collaboration (NRC/NAS 2001, p. 184).

The director of the TRUST project said something along the same lines in his testimony before Congress. He said that a fundamental organisational problem is the lack of mechanisms for filling in the gap between the end of a successful federal research programme and the investment by the venture community and industry in products. He added that industry, especially systems integrators and the larger IT companies, would benefit from roadmaps informed by this technology transition (Sastry 2003).

Among the noteworthy platforms (=alliances, associations, lobby groups) which we have reviewed for this chapter and which are focused on ubiquitous computing and/or privacy and related issues are the following:

ZigBee Alliance

The ZigBee Alliance[50] 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. As of April 2005, the ZigBee Alliance had about 150 members. Membership is open. ZigBee says it is the only standards-based technology designed to address the unique needs of low cost, low power, wireless sensor networks for remote monitoring, home control, asset management and building automation network applications in the industrial and consumer markets. ZigBee provides a security toolbox approach to ensure reliable and secure networks.

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),[51] developed by the World Wide Web Consortium, is emerging as an industry standard

[50] www.zigbee.org

[51] 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. At its most basic level, P3P is a standardised set of multiple-choice questions, covering all major aspects of a Web site's privacy policies. Taken together, they present a snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P-enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences.

There are quite a few papers on the P3P website, the vast majority of which date from 2002 and before. One of the papers (one of the most recent!) is the summary report of the W3C Workshop on the Future of P3P, held in November 2002.[52] Among other things, the report notes that there are some disclosures required by the EU privacy directive (95/46) that are not accommodated by the P3P vocabulary. There is no element to explain to which jurisdiction data are going, no element to explain a company's security practices, and no element to describe the maximum data retention period. P3P does not address all of the FTC's Fair Information Principles.

Former FTC commissioner Christine Varney expressed her view that the original goal of P3P was to let technology take a lead in addressing online privacy issues and identify areas for regulation where technology fails. She said she believes P3P policies have legal consequences and that sites that misrepresent themselves in either their P3P policies or their human-readable policies might be prosecuted for deception.

The Platform for Privacy Preferences (P3P) 1.0 Recommendation was issued in April 2002 after five years of intense development. In February 2004, the P3P specification working group published a first public working draft and subsequent revisions of the P3P 1.1 specification. The group expects to issue a last call before July 2005.

Liberty Alliance

The Liberty Alliance[53] has a membership of more than 150 companies, non-profit and government organisations from around the world. The consortium is developing an open standard for federated network identity that supports all current and emerging network devices. The Alliance says that federated identity offers businesses, governments, employees and consumers a convenient and secure way to control

[52] www.w3.org/2002/12/18-p3p-workshop-report.html

[53] www.projectliberty.org

identity information in today's digital economy, and is a key component in driving the use of e-commerce, personalised data services, as well as web-based services.

TRUSTe

TRUSTe[54] is an independent, non-profit organisation dedicated to enabling individuals and organisations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. TRUSTe was founded in 1997 by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium to act as an independent, unbiased trust entity. Sponsors include AOL, Intuit, Japan Engineers Foundation and Microsoft. The TRUSTe privacy program – based on a branded online seal, the TRUSTe "trustmark" – bridges the gap between users' concerns over privacy and Web sites' needs for self-regulated information disclosure standards. By awarding the trustmark, TRUSTe recognises companies that are doing the right thing in online privacy.

In April 2005, TRUSTe issued its first set of data security guidelines to assist companies in evaluating new or existing policies for protecting consumer and employee personally identifiable information (PII).

TRUSTe says its privacy certification and seal programme complies with the EU Safe Harbour Framework. 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)[55] is a public interest research centre in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment and constitutional values. EPIC is funded by individual contributors, private foundations and companies. It also generates some income from litigation and the sale of publications. It litigates Freedom of Information Act, First Amendment and privacy cases. It publishes books on open government and privacy.

It claims to maintain one of the most extensive web sites on privacy and free speech issues on the Internet. It publishes an online newsletter and provides an extensive listing of privacy resources. Among its new challenges, EPIC says that RFID privacy is a big issue. It does not object to the use of RFIDs for inventory management, but

[54] www.truste.org

[55] www.epic.org

objects to tagging people. 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. It understands the need to detect threats to public safety, but says open-ended programmes of mass public surveillance must be reined in. It is working with the University of Ottawa Law School on a project to promote technologies for privacy.

2.3.6 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. Many projects, as in Europe, are collaborative efforts of different partners. Some of the projects, such as Oxygen, are supported by partners from outside the United States.

Several important and well-known projects are mentioned in this section. Reference is made to others in the sections that follow on the issues of privacy, identity, security, trust and the digital divide.

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,[56] 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.

Among the commercial spin-offs from the project is Dust Networks[57], whose co-founder and chief technology officer is Kris Pister, who was in charge of the project at Berkeley. Dust Networks combines its wireless mesh networking software and low-power wireless nodes for monitoring and control applications, such as building automation, industrial monitoring and security services. Another is Crossbow Technology Inc[58] which claims to be the leading “full solutions” supplier in wireless sensor networking and the only manufacturer of smart dust wireless sensors. Crossbow’s open TinyOS architecture enables intelligent multi-sensing devices to dynamically self-organise to capture and send data anywhere.

[56] http://robotics.eecs.berkeley.edu/~pister/SmartDust/

[57] www.dust-inc.com/company/team.html

[58] www.xbow.com/General_info/AboutCrossbow.htm

Similar in concept to the Smart Dust project is **Smart Matter**, a project at the Palo Alto Research Center (PARC), a subsidiary of Xerox Corporation. Xerox conducts research with strategic partners to commercialise technologies created by its scientists. Marc Weiser coined the term ubiquitous computing in 1988 while an employee at PARC. PARC's Computer Science Laboratory continues research in ubiquitous computing.

PARC's Smart Matter project began in the late 1990s, underpinned by micro-electro-mechanical systems (MEMS) which make it possible to mass produce large numbers of integrated sensors, actuators, computers and communication systems that can be embedded within products or spread throughout the environment. The Smart Matter concept is based on the notion of programmable matter, so that fundamental properties such as shape, stiffness, colour, reflectivity of light and sound, and even load-bearing strength can be dynamically adjusted on demand.

PARC is also carrying out privacy and security research. Its Computer Science Laboratory recognises that with advances in aggregating and mining data and the trend toward ubiquitous computing, the potential for privacy violations continues to increase. PARC is developing protocols which, it says, "finesses" the tension between the efficiency and functionality of systems and privacy. Technologies developed by PARC are based on two key premises:

- Security requirements should be inferred from user actions.
- Users should be provided useful and convenient ways to control their security environment.

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.[59] CENS researchers are investigating fundamental properties of embedded networked sensing systems, developing new enabling technologies and exploring novel scientific and societal applications.

Although most of its research is technical, CENS is also studying the ethical, legal and social implications of the new technology. CENS researchers believe that not only is it possible to embed values in the design of information technologies, it is impossible not

[59] 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.

to do so. For example, choices on whether user authentication will be required for transactions have large implications for privacy and security. Consequently, for embedded networked sensors, it is important to consider exactly which values are to be embedded and the process by which this may occur. [60]

Oxygen is a big, well-funded ($50 million) project (2000-05)[61] at the Massachusetts Institute of Technology (MIT) sponsored by Acer and Delta Electronics, Inc. (Taiwan), Hewlett-Packard Corp. (USA), NTT (Japan), Nokia Research Center (Finland), Philips Research (Netherlands) and DARPA. Oxygen is an integrated software system that enables pervasive, human-centred computing through a combination of specific user and system technologies developed for use in the home, at work or on the move. The Oxygen goal was to make computation and communication as natural to use as the air we breathe.

MIThril is a next-generation wearables research platform[62] developed by researchers at the MIT Media Lab. The MIThril project has been developing and prototyping new techniques of human-computer interaction (HCI) for body-worn applications since about the year 2000. Through the application of human factors, machine learning, hardware engineering and software engineering, the MIThril team has been constructing a new kind of computing environment and developing prototype applications for health, communications and just-in-time information delivery. The project team recognises that wireless data links raise privacy concerns. Strong cryptography would probably be needed to make a wireless body-LAN private, but this would impose additional computational (and thus power) overhead. They say that what is really needed is a short-range, low-power, ad-hoc, peer-to-peer, wireless networking protocol that could support device and resource discovery, authentication and transparent data encryption. Research continues.

The **Aware Home** Research Initiative (AHRI)[63] is an interdisciplinary research project at the Georgia Institute of Technology which centres on a three-story home that

[60] http://research.cens.ucla.edu/portal/page?_pageid=56,49653,56_49655&_dad=portal&_schema=PORTAL

[61] www.oxygen.lcs.mit.edu/index.html

[62] The project started in about the year 2000 and continues. Its website is www.media.mit.edu/wearables/mithril/overview.html

[63] The laboratory was funded by a $700,000 grant from the Georgia Research Alliance. It also received funding from a consortium of more than 20 information technology companies as well as the NSF. The project began in 2000 and is continuing. Its website is www.awarehome.gatech.edu.

functions as a living laboratory for interdisciplinary design, development and evaluation. In addition to the research on the design and application of suitable home technologies, the project explores the social, political, legal and economic benefits and concerns related to privacy and autonomy when services exploit awareness and knowledge of human activity within the protected space of a home. Researchers have built an environment that can sense the inhabitants through a variety of technologies, including video, audio, motion and load. One result of the project is the finding that older adults are willing to give up some privacy if it enables them to remain independent longer (Becker 2004).

The **Portolano** project[64] 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.[65] 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.

One of the Portolano projects is called *one.world,* a system architecture that provides a framework for building pervasive applications. Although the researchers say they have validated their architecture, security for pervasive computing environments – specifically the authentication of users, devices and applications – remains an open issue (Grimm et al. 2004, p. 424).

[64] http://portolano.cs.washington.edu. Portolano takes its name from the seacoast charts created by Portuguese sailors of the 14th and 15th centuries. They were fundamental to the Age of Discovery initiated by Portugal's Prince Henry the Navigator that led to the European discovery of the African coast and the New World.

[65] Donald Norman was an executive at Apple Computer and Hewlett Packard. He also taught cognitive science and psychology at the University of California, San Diego and computer science at Northwestern University, and wrote several books on design. 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.

2.3.7 Privacy

The *Embedded Everywhere* report made several recommendations with regard to privacy:

- Systems should be designed to incorporate a wide range of potential privacy policies.
- Owing to the passive and ubiquitous nature of many of these systems, users will often not be aware that information about them is being gathered. Notifying users who may not even be aware of the existence of the EmNet is a difficult problem. Even more difficult is acquiring meaningful informed consent from those users. Research into these and related issues is essential.
- Research into possible legal requirements for the protection of personal information may be needed to ensure adequate accountability. The goal should be to ensure that specific individuals or agents, probably those who deploy EmNets and will use the information gained therefrom, are deemed responsible and accountable for the protection of an individual's private information collected on those networks. Accountability, like privacy, is not absolute. What is needed is technology to support a range of preferences, which may vary with users and contexts, for enhancing privacy, accountability and other values.
- Research in designing systems whose default policy is to preserve individual users' anonymity is needed. It is an open question to what extent these systems would need to allow completely untraceable use rather than just strict identity protection except in the presence of authorized agents. Another possible avenue of investigation would be to enable anonymity-preserving authentication -- for example, to enable systems to determine that individuals are members of a certain group (say, doctors in a hospital) but not to allow more fine-grained identification (NRC/NAS 2001, p. 139).

Privacy, security, identity and trust issues form a strong undercurrent in many ubiquitous computing projects in the United States, as those mentioned above indicate. A much smaller number are specifically focused on privacy. The **PORTIA** project[66] is one of those. It is addressing both the technical challenges of handling sensitive data and the policy and legal issues. It is a five-year, multi-institutional, multi-disciplinary,

[66] PORTIA is the acronym for Privacy, Obligations, and Rights in Technologies of Information Assessment. The project is funded by the National Science Foundation under the Information Technology Research Program. http://crypto.stanford.edu/portia/

multi-modal investigation that looks comprehensively at sensitive data in a networked world. There are two main academic centres of activity (Yale and Stanford). Project participants are studying techniques for meeting the potentially conflicting goals of respecting individual rights and allowing legitimate organisations to collect and mine massive data sets. Because technical goals are affected by lack of agreement about the meanings of basic terms, most notably “privacy”, another major PORTIA goal is the development of a conceptual framework for the study of rights, responsibilities and public policies focused on sensitive-data handling. The conceptual framework is built on the notion of “contextual integrity”, which considers both the context and content of data in assessing sensitivity.

The **SHARP** project (System for Human Activity Recognition and Prediction) is also exploring the what and how of context-aware computing, which leverages recent advances in sensors, machine learning and data mining to create ubiquitous computing systems. The SHARP project is a collaborative effort of Intel Research Seattle and the University of Washington. Intel has a research interest in emerging and disruptive technologies that will enable a future of proactive computing.[67] Intel says it is working against an Orwellian future and towards “a pleasantly proactive future” by grappling the tough trade-offs between privacy and utility, and automation and annoyance.

The goal is to build a system that can automatically infer a wide range of everyday human activities (such as cooking pasta, taking a pill, or washing dishes) and provide proactive assistance, if needed, to complete an activity. One broad objective of the project is to enable the elderly to continue living in their homes for as long as possible.

Machine learning systems vary, but all have three main components:

- Sensors that gather data about the physical world. In the case of SHARP, RFID tags gather data about which objects are being used to perform an activity, and additional sensors are used to capture other data, such as motion, temperature or visible light.
- Models or prior knowledge about real-world processes or human activities.
- A reasoning engine or machine learning algorithm which analyses sensor data, compares it to a large set of models, infers which model is the closest match for the data, improves the models based on observed data, and recommends appropriate actions.

[67] www.intel.com/research/areas.htm

Projects such as SHARP show that sensor networks are getting better at understanding human behaviour. While such programs have obvious benefits as outlined by SHARP, it is easy to conclude that they also have significant potential for surveillance and invasion of privacy.

IBM has undertaken several privacy projects under the auspices of its **Privacy Research Institute**, which it says is the industry's first technology research institute devoted to privacy.[68] The institute's goal is to develop the necessary technologies for enterprises that enable the transition from today's privacy-unaware or even privacy-intrusive ways of doing e-business to privacy-enabling ways.

One of the institute's privacy-related projects is called **SPARCLE**, the aim of which is to enable privacy professionals in any industry to author policies, translate these policies into system readable commands, implement them with an enforcement engine and run reports to monitor the effectiveness of the policy implementation. The compliance checking functionality in SPARCLE allows organisations to run reports to understand what data accesses are being allowed and denied by the policy.

While IBM's Privacy Research Institute works away on technologies to protect privacy, a different part of the IBM organisation is working on projects aimed at keeping track of customers. One such project is called **Margaret** (Ward 2004). IBM has been working on a customer identity concept based on putting RFID tags into passbooks, wallets or cards. When a customer passes through the doors of a bank, the card would alert a customer information system. Customers could then be greeted by name by tellers, who would already have their account information on-screen when they arrive at the counter.

Yet another part of IBM offers marketing and customer intelligence "solutions".[69] It offers what it calls "Web analytics", which tracks Web traffic and customer preferences, enabling IBM's corporate customers to initiate cross-sell and up-sell opportunities, and data-driven personalisation, providing a real-time marketing ability to "synch online and offline transaction data to build a comprehensive customer view."

IBM's **PeopleVision** project is developing systems that understand human motion using video cameras. One of the main systems is the Smart Surveillance Engine – a software system which can "watch" surveillance video and automatically detect alert conditions such as abandoned objects or intrusions. The software comes with a

[68] www.research.ibm.com/privacy/

[69] www-1.ibm.com/solutions/businesssolutions/doc/content/solution/972941107.html

searchable "Smart Surveillance Index" that can be browsed or queried to quickly find interesting events in stored data. The system can be tailored to control the amount of information presented or obscured. Access controls specify which users are able to observe which components of a video stream.

2.3.8 Identity

The US Federal Trade Commission estimates that more than 10 million Americans are victims of identity theft every year, which imposes a cost of about $5 billion on individuals and $48 billion on businesses.

In response to the human and financial costs of identity theft, a variety of policy responses have been proposed. Most recognise the necessity of a multi-pronged effort involving the public and private sectors and employing legal and technological tools. Education of consumers is essential to ensure that they take steps to minimise the possibility of identity theft and to alert them to signs of possible theft. Public and private organisations can help prevent identity theft by reducing the amount of data that is exposed, limiting the release of information that is given at the point of service, and enhancing the security of data that are collected. Additionally, aggressive criminal investigations, prosecution and punishment are critical (Kent/Millett 2003, p. 100).

The *Who goes there?* report's concluding chapter provides a toolkit that can aid in designing an authentication system sensitive to privacy concerns (Kent/Millett 2003, pp. 179ff). It focuses on the three types of authentication:

- *Individual authentication* is the process of establishing an understood level of confidence that an identifier refers to a specific individual.
- *Identity authentication* is the process of establishing an understood level of confidence that an identifier refers to an identity. The authenticated identity may or may not be linkable to an individual.
- *Attribute authentication* is the process of establishing an understood level of confidence that an attribute applies to a specific individual.

The choice between attribute, identity and individual authentication systems bears substantially on the privacy consequences. Attribute authentication systems present the fewest privacy problems and individual authentication systems the most. When an authentication system is developed, decisions will need to be made about which attributes to use, which identifiers will be needed, which identity will be associated with the identifier, and how the level of confidence needed for authentication will be reached.

The report recommends that, to better protect information privacy (and in accordance with fair information principles), once an attribute is selected, individuals should receive clear notice about whether information regarding that attribute will be retained in a separate authentication system of records, what the uses of that system are, who has access to it, and what rights the individual has with respect to accessing the system. The system should also specify how controls on the attribute authentication system will be enforced and to whom the system is accountable.

In June 2005, the Liberty Alliance announced formation of a new multi-organisational group to combat identity theft. The Identity Theft Prevention Group is designed to serve as a hub for the global effort against identity theft, attacking these issues from multiple fronts in a collaborative, open and vendor-neutral environment. “The first step in solving any difficult problem,” said a Liberty spokesman, “is defining and establishing the scope of the issue. Our team is working on this now, analyzing this problem from every angle and painting a clear picture of what we are up against. From this, we’ll be able to provide a comprehensive view of the issues and threats, recognize behaviors that put organizations and consumers at risk, and present specific guidance on avoiding these actions.” Liberty says the only truly effective solution is a balanced approach of technology and strong policy practices, as well as an educated public. Liberty’s goal is to work with its partners to introduce best practices and educate consumers and businesses, providing them with the tools they need to make informed decisions. Liberty promotes a federated network identity approach to deliver the benefit of simplified sign-on to users by allowing users to “link” elements of their identity between accounts without centrally storing all of their personal information. With a federated network identity approach, users authenticate once and still retain control over how their personal information and preferences are used by the service providers, regardless of the device or network access method. Liberty is hosting its first Identity Theft Workshop in Chicago in July 2005. This workshop will bring together government agencies, consumer groups and industry working on various identity theft issues to analyse some of the most pressing online identity theft problems.[70]

2.3.9 Trust

Different approaches to trust have been considered in the United States. One of the more interesting is that developed in the **AURA** project[71] at Carnegie Mellon University

[70] www.projectliberty.org/press/details.php?item_id=116

[71] 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.

(CMU), the goal of which was “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 (Garlan et al. 2002).

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. A person's current location is a sensitive piece of information, which only authorised entities should be able to learn. Several challenges arise in the specification and implementation of policies controlling access to location information. There can be multiple sources of location information, the sources can be within different administrative domains, different administrative domains might allow different entities to specify policies, and policies need to be flexible. CMU scientists address these issues in design of an access control mechanism. Their design encodes policies as digital certificates (Hengartner/Steenkiste 2004). They also plan to investigate whether their ideas can be applied to protect other kinds of information in a ubiquitous computing environment.

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[72], 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”.

[72] 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

Privacy, legal, societal and usability issues will be built into the technology as it is developed rather than added on as an afterthought.

The previously mentioned Oxygen project has focused on trust as well and, in particular, on self-certifying (SFS) and co-operative (CFS) file systems providing secure access to data over untrusted networks.

2.3.10 Security

The US government drive to increase support for fundamental research in cyber security was abetted by a March 2005 report from the President's Information Technology Advisory Committee (PITAC 2005) which said that the “information infrastructure of the US is highly vulnerable to disruptive domestic and international attacks.” One big cyber security project into which the US government has put money is at the University of California-Berkeley. Called **DETER** (Cyber Defense Technology Experimental Research network), the project provides a testbed for network defence.[73] Berkeley put together a coalition of partners to create and operate a researcher- and vendor-neutral experimental infrastructure which simulates the makeup and operation of the Internet, from routers and hubs to end users' computer desktops. The testbed serves as a shared laboratory where researchers from government, industry and academia can put their cyber security technologies to the test. The network is intentionally challenged by malicious codes that range from worms to denial-of-service attacks to programs that attack a network's routing infrastructure.

2.3.11 Digital divide

We found no ubiquitous computing projects in the United States which focused on digital divide issues.

2.3.12 Safeguards

From our review of the research on ubiquitous computing in the US, we found various types of safeguards. Among them are the following:

[73] The partners include the University of California Davis, University of Southern California-Information Systems Institute, Network Associates Laboratories, SRI, Menlo Park, Pennsylvania State University, Purdue University, Princeton University, University of Utah, and industrial partners Juniper Networks, CISCO, Intel, IBM, Microsoft, and HP. The three-year project (2003-06) received $10.8 million from the US National Science Foundation and the Department of Homeland Security (DHS). The project’s website is www.isi.edu/deter. See also www.berkeley.edu/news/media/releases/2003/10/15_testbed.shtml

Privacy policy standards

Currently, there are a wide range of privacy policies on corporate Web sites. Some aren't worth the cyber ink they've been written with. Often they are too long, written in legalese and don't provide any options to the prospective customer. The Platform for Privacy Preferences Project (P3P) has made some progress towards a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. P3P supposedly enhances user control by putting privacy policies where users can find them, in a form they can understand and enables them to act on what they see. While P3P was written for today's Web (or, at least, the Web as it was pre-2002), it can be considered as a useful starting point for the emerging Internet of things.

P3P allows companies to make privacy promises, but additional tools are needed to help enforce these promises. The snag with P3P is that it puts the onus of safeguarding privacy in the hands of organisations that are often themselves guilty of trespass or sloppiness. A case can also be made for organisations to leave control in the hands of individuals.

Identity management protocols

Identity management protocols offer a good safeguard, if they do what they are intended to do. The Liberty alliance has developed specifications for federated identity and web services built on an open protocol called Security Assertion Markup Language (SAML), which it describes as device and platform "agnostic". Liberty collaborates with other standards bodies such as the Organization for the Advancement of Structured Information Standards (OASIS), which approved SAML 2.0 as a formal draft in March 2005. Liberty plans to start testing tools that incorporate SAML 2.0 in the summer of 2005.

IBM has also been developing cross-domain web identity authentication protocols. IBM says the security of browser-based federation protocols, including Microsoft Passport, the Liberty/OASIS SAML, and Web Services Federation Language (WS-Federation), is still unproven. IBM has developed a browser-based attribute-exchange (BBAE) protocol, which it says is more privacy-friendly and scales better to multiple enterprise federations without any single point of control. According to IBM, its protocol provides authenticity and secure channel establishment in a realistic trust scenario.

IBM has developed other identity management tools too. Researchers at its Zurich Research Laboratory in Rüschlikon, Switzerland, operate on the principle of "data parsimony." The basic concept is that personal data are best protected if the amount of data revealed is kept to a minimum. The **"idemix**" system developed in Rüschlikon uses pseudonyms for e-commerce transactions. Under "idemix", a user would first select a pseudonym, then register using this pseudonym and receive the corresponding credentials with an electronic signature. If later the user wants to access the service, he or she must only first provide proof to the service that the corresponding, digitally signed credentials are in his or her possession. By employing modern cryptographic techniques, the so-called Zero-Knowledge proofs, researchers at IBM propose that a pseudonym and credentials be given to the online service only in encrypted form. Although the online service cannot decrypt the information, it can still employ a clever interaction tactic with the user to verify the authenticity of the encrypted pseudonym. Because a new encryption is used every time, the repeated use is hidden from the online service, i.e., the user is not re-identified and thus can act completely anonymously. However, for many applications, this total anonymity is undesirable: for example, if a rented car is not returned, the identity of the person who rented the car has to be retrievable. Therefore, the idemix system makes provision for a designated authority who can uncover such an identity.

Procedural safeguards

Procedural safeguards can be employed to protect privacy, which would be the case if RFID tags are “decommissioned” at the retail counter so that they are no longer functional when customers leave a store.

Liability and insurance

The insurance industry has a role to play in protecting privacy and preventing identity theft. If companies are made liable for breaches in their securing personal data, then they will seek insurance to offset that liability. Before providing such insurance, the insurance companies will want to make sure that prospective clients have taken requisite measures to protect the data they hold.

Media attention

Threats to privacy and identity theft have become important public issues in the United States, helped by stories in the press[74] (especially stories involving the data warehousing, data mining and profiling activities of companies such as Acxiom, ChoicePoint, LexisNexis, Seisint, Verint, etc as well the government’s surveillance

[74] For example (Dash/Zeller 2005): “MasterCard International reported yesterday that more than 40 million credit card accounts of all brands might have been exposed to fraud through a computer security breach at a payment processing company, perhaps the largest case of stolen consumer data to date.”

activities under the Total Information Awareness and CAPPS II[75] programmes). Reports from the National Academy of Sciences and recent books such as *The Digital Person* by Daniel J Solove and *No Place to Hide* by Robert O'Harrow have also served the public interest by documenting how personal information is being abused by both the government and the corporate sector. Such unwanted publicity may be expected to lead to better practice in government and in the private sector in terms of privacy protection. However, what is really needed is some new legislation.

Legal and regulatory safeguards

The United States has not adopted legislation comparable to the data protection directive (95/46/EC) or the privacy and electronic communications directive (2002/58/EC) in Europe to build in safeguards for the protection of personal information. Indeed, the USA PATRIOT Act and other such legislation work at cross-purposes to the protection of privacy and increase the scope for surveillance of the citizenry.

Some state governments, however, are passing new legislation (e.g., California law SB1386, effective July 2003) that forces organisations to inform individuals whenever there has been a privacy breach, and makes organisations liable for improper use of information.

Guidelines

US researchers have proposed several sets of guidelines aimed at protecting privacy and avoiding identity theft. Such guidelines are helpful as safeguards, but, of course, they are by themselves insufficient to ensure privacy truly is protected. Guidelines will not stop someone intent on violating privacy.

One set of guidelines can be found in the *Who goes there?* report. It recommends that, when designing an authentication system or selecting an authentication system for use, one should:

- Authenticate only for necessary, well-defined purposes;
- Minimise the scope of the data collected;
- Minimise the retention interval for data collected;

[75] CAPPS II is the acronym for Computer Assisted Passenger Prescreening System, a computerised database used to profile individuals to determine their threat level when flying. The government has not released details about what information is gathered or how people are profiled, nor do passengers have the ability to challenge their classification.

- Articulate what entities will have access to the collected data;
- Articulate what kinds of access to and use of the data will be allowed;
- Minimise the intrusiveness of the process;
- Overtly involve the individual to be authenticated in the process;
- Minimise the intimacy of the data collected;
- Ensure that the use of the system is audited and that the audit record is protected against modification and destruction; and
- Provide means for individuals to check on and correct the information held about them that is used for authentication (Kent/Millett 2003, p. 78).

One of the papers available for downloading from the Liberty website is on Privacy and Security Best Practices (Varney et al. 2003). The document highlights selected national privacy laws, fair information practices and implementation guidance for organisations using the Liberty Alliance specifications. Topics addressed include adoption and implementation of privacy policies, notice and disclosure, choice and consent, data quality, security safeguards and accountability.

TRUSTe provides tools to increase trust between digital businesses and their customers. According to TRUSTe, there are 10 high-level requirements every company should consider implementing in order to achieve reasonable security protections of personal or sensitive data:

- An enterprise-wide data security policy and employee training program
- Internal control over the collection, use and sharing of confidential or private data
- Access procedures that are based on an individual’s “need to know”
- Internal control over the management of third-party vendor or outsourced relations
- Administrative control and physical security
- Perimeter controls, such as firewalls and VPNs
- Encryption of sensitive data sent across public networks, especially when using wireless or Bluetooth technologies
- Updates for anti-virus software and security patches
- Identity management and authentication procedures (when feasible)

- Regular tests and monitoring.[76]

EPIC also provides a guide to practical privacy tools. However, most of those tools[77] are for use in conjunction with today's Internet, rather than the Internet of things which is developing rapidly as the cost of RFIDs and "smart dust" technologies drop towards earth.

Trustmarks

A trustmark could also be a useful safeguard of sorts. Operators or service providers or others who collect personal or sensitive data would be allowed to post a trustmark certifying that they comply with industry-wide accepted best practice. One such trustmark is that awarded by TRUSTe which claims to be the most widely used. By awarding the trustmark, TRUSTe recognises companies that are doing the right thing in online privacy.

2.4 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.

2.4.1 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 first of the dozen or so NRI Papers came out in 2000. Evidence would suggest they have been very influential. It is no accident that the Ministry of Internal Affairs and Communications (MIC) 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. If the title on the cover is somewhat fanciful, the pages that follow are earnest and well thought out.

The NRI Papers

[76] www.truste.org/about/securityguidelines.php

[77] A long list of such tools can be found at www.epic.org/privacy/tools.html

Nomura Research Institute (NRI) is a leading think-tank and systems integrator in Japan, amongst whose clients are government organisations, private companies in financial, manufacturing, retail and other industries in Japanese and foreign markets. Nomura has published about a dozen papers on ubiquitous networking in Japan.[78] They are cogent, thoughtful and strategic. Several were authored by Teruyasu Murakami.[79] Perhaps the most important is one entitled "Establishing the Ubiquitous Network Environment in Japan – from e-Japan to u-Japan" which was published in July 2003.

In his paper, Mr Murakami proposes a u-Japan strategy which, one can assume, caught the eye of the Ministry of Internal Affairs and Communications and led to his appointment as chairman of the MIC's policy roundtable in March 2004. As noted in the section on u-Japan below, the roundtable was tasked with preparing a policy package for realisation of a ubiquitous network society in 2010.

Mr Murakami says that there is no doubt that the concept of the ubiquitous network will continue to shape the core trends in technological development, business development and the structuring of social systems. He sees ubiquitous networking as an IT environment that can create a new market of ubiquitous electronics and services in which diverse and profuse digital content is exchanged through connections to broadband networks. These networks, which provide constant access, include not only wired systems but also wireless and mobile systems, and they use Internet protocols (IPv6 as much as possible) to handle a constant exchange of information between personal computers, mobile telephones, PDAs, digital TVs, home information appliances, game machines, car navigation systems, vending machines, Web cameras, RFID tags, and even equipment and products that were not previously regarded as information equipment.

He says NRI created the concept of the ubiquitous network (Murakami/ Fujinuma 2000). He defines the ubiquitous network from a supplier's point of view as an IT environment that meets the following requirements:

[78] www.nri.co.jp/english/opinion/papers/index.html

[79] Mr. Murakami is a Managing Director of Nomura Research Institute. He joined NRI in 1968 and became a member of the Board in 1996. He is also Director of the Tokyo Club Foundation for Global Studies and acting as chairman of Electronic Commerce Promotion Working Group of Nippon Keidanren and Business Steering Committee Member of GBDe (Global Business Dialogue on electronic commerce). He has written and edited numerous books and papers in English and Japanese, including "Ubiquitous Networks," "The Emergent Creation of New Industries," "Future Perspectives for Cyber Society," "Social and Economic Systems in the Network Century" and "Future Sprouts."

- It provides broadband network access with mobility to allow for always-on connections regardless of the place of usage and incorporating such modes as fixed and mobile, wired and wireless systems, or communications and broadcasting;
- It allows for connecting not only large-scale general-purpose computers and personal computers, but also mobile telephones, PDAs, etc;
- It enables the utilisation of content that involves not only text, data and still images, but also the transmission of animated images and sound, as well as the utilisation of solutions satisfying the pressing needs of users and the utilisation of platforms that enable secure exchanges of information and the implementation of commercial transactions.

He says a definition should include what the ubiquitous network looks like from the viewpoint of the user:

- The user sees the ubiquitous network as an IT usage environment that provides access to a broadband network from literally anywhere;
- The ubiquitous network provides constant access;
- On the ubiquitous network, the user can handle all manner of content.

From the user's perspective, a ubiquitous network describes an IT usage environment in which almost anything (with a tag attached) can be connected to the network, anywhere and at any time.

Mr 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).

He distinguishes also 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 (Kato et al. 2004)[80] 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 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 (Kato et al. 2004, p. 60).

The report is based on 10 visions and concepts targeted by future mobile communications systems that serve as the foundation of studies performed by the Mobile IT Forum (see below for more on the mITF). Business models and technologies needed for realising the visions were considered in the report. The report also contains studies on user expectations and technical requirements. Privacy protection is stated as one of the requirements.

4G is envisaged for commercial introduction by 2010, which is the same date targeted by the Ministry of Internal Affairs and Communications (MIC) for the ubiquitous network society. Assessments and expectations by the users, society and industry are explored in the *Flying Carpet* report based on “images” of future mobile communications services. The report provides a “functional” roadmap towards 4G mobile systems.

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” (Kato et al. 2004, p. 50). 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.

Elsewhere, the report says that according to its survey, privacy protection ranked higher among users than other 4G features. The report notes that it is necessary to

[80] 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

establish a framework for the provision of services to users based on their location, but in a way that protects their privacy and provides a mechanism for controlling unwanted advertisements.

In the transition to 4G, personal information is stored on user terminals or IC cards and biometrics are or will be used for authentication in the 2005-2006 time frame. However, with the arrival of 4G, “a lot of personal information is managed on the network” and authentication will be unnoticed by users.

Why would we want “the network” to manage any more personal information than it already does? Perhaps the answer is supplied somewhere else in (on?) the *Flying Carpet*. The report says that in the 4G world “the information environment for users is expected to become increasingly complex.” How is that solved? By means of “an intelligent information collection and management support feature (personal agent), which selects information catered to users’ individual needs, and automatically stores and associates them”. This personal agent, says the report, will become indispensable. (The personal agent concept is somewhat similar to the Personal Well-being Assistant envisaged by the Dutch Embedded Systems Roadmap.) It will estimate our intentions and present “optimal” information in an optimal fashion (Kato et al. 2004, p. 62). Optimal for whom, one wonders. Who decides what is optimal? The report goes on to say that “it is required to have an intelligent search system, which, for example, present user’s past search instructions/results, records user’s degree of satisfaction vis-à-vis the outcome of the search, and automatically learns from such practice.”

The report envisages a single sign-on for connection to ubiquitous networks using biometrics (e.g., a fingerprint) (Kato et al. 2004, p. 107). Authentication and security are one of the most important requirements of users as well as service providers and operators in the 4G environment, but, says the report, it is also important to avoid causing excessive burdens for the users for the sake of security. The user ID and password-based authentication used today are too burdensome; a more secure and burden-free authentication method is needed for 4G (Kato et al. 2004, p. 61). The use of PKI and biometrics (fingerprints, voice prints, retinas, irises) are assumed for authentication.

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 Ministry of Internal Affairs and Communications (MIC)[81] established a “policy roundtable”[82] in March 2004 to investigate a concrete form and a policy package for realisation of a ubiquitous network society in 2010. The roundtable considered the broad design of a ubiquitous network society, measures for its realisation and measures to remedy areas that fall into the dark side of the ubiquitous network society. The policy roundtable published its final report in December 2004.[83]

The policy roundtable’s report appears not to have been translated yet into English, although a summary of the report exists in the MIC’s biweekly newsletter (MIC 2005). The u-Japan policy is built on three pillars or goals:

1. *Preparation of ubiquitous networks*

A seamless network environment, including wire and wireless communications, networks and terminals, authentication, data exchanges, etc., shall be prepared. By 2010, 100% of Japanese nationals will have access to high-speed or ultrahigh-speed networks.

2. *Advanced use of ICT*

In order to provide solutions to problems in medical care, social welfare, disaster prevention, public security, education, human resources development, etc. in the 21st century, the use of ICT shall be advanced. In the year 2010, 80% of Japanese nationals shall recognise that ICT provides effective solutions to social problems.

3. *Preparation of an environment for ICT use*

MIC will (i) implement the "ICT Safety and Security 21 Strategy" for reducing security concerns accompanying the ICT penetration, (ii) formulate the "Charter of Ubiquitous Network Society" as guidelines for providing solutions to "negative" aspects of the ubiquitous network society, and (iii) transmit the u-Japan approach to the rest of the world.

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.

[81] 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

[82] Chaired by Teruyasu Murakami, Nomura Research Institute.

[83] www.soumu.go.jp/s-news/2004/041217_7.html. It is interesting to note the people-centred aspect of the vision of a ubiquitous network society as opposed to simply a ubiquitous network.

With respect to the international community, the policy roundtable urged MIC to (i) make Japan the frontrunner in the ICT field, (ii) advocate u-Japan concepts and declare the "Charter of Ubiquitous Network Society," and thereby (iii) contribute to realisation of a society in which people around the world can enjoy their lives through safe and secure use of ICT.

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" (MPHPT 2004). The White Paper is quite wide-ranging. It reviews advances in Japan's network infrastructure (broadband, mobile and wireless networks, Internet, etc), changes in lifestyles, business use of networks, social issues, ICT trends, the telecoms and broadcasting business, content, human resources development, R&D, trends in the US, Europe and Asia. It sets out a strategy for u-Japan, covering policy development, upgrading ICT networks, promoting the concept in the private and public sectors, promoting R&D and international strategies. There is also a section on protecting information and communications users, backed up by some earlier discussion of the results from a survey.

The White Paper says that realisation of ubiquitous networks will enable anyone to access and exchange information of any kind freely at any time from anywhere, and from any appliance. Japan will promote international standardisation of ubiquitous network technologies. It also says Japan must undertake measures to ensure information security.

The White Paper provides an indication of people's expectations of ubiquitous networks. There is quite an interesting ranking of services that respondents indicated they would use which were generated from a survey of personal activities in a ubiquitous network society (MPHPT 2004, p. 18). 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" (MPHPT 2004, p. 31).[84] Experts

[84] There are few details in the White Paper about the survey, who carried it out, who sponsored it, when it was carried out, how many people were surveyed, etc. The MPHPT also prepared a pictographic version of the White Paper for the overseas press: http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2004/press_information01.pdf

in the field were asked about problems that had to be overcome. Common responses were “ease of use and understanding” (human-computer interfaces that anyone can use) and “security and safety” (structures to prevent improper use of personal information, theft of money, etc.).

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 (MPHPT 2004, p. 32).[85]

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.

To ensure information security, the White Paper says, organisational steps should be taken inside and outside companies, an improvement both in the awareness and knowledge of employees and their information literacy, the formulation of security policies, and regular implementation of information security audits, and security measures at the operational and organisational levels (MPHPT 2004, p. 35).

Since there are no actual borders to information and communications networks, it is possible that an attack on networks will go beyond one country to cause increasing damage. The White Paper notes that the Council of Europe adopted the “Convention on Cybercrime” in November 2001. So far, 37 countries, including Japan, have signed the convention but only five have ratified it.

[85] Although the White Paper does not provide details, the incident involved theft of Yahoo BB’s customer database. In February 2004, Tokyo police arrested three men for trying to extort 3 billion yen (U.S. $28 million) from Softbank and seized DVDs and CDs that contained the entire Yahoo BB customer database. Yahoo BB (Broadband) is the leading DSL and IP telephone service provider in Japan, owned and operated by Softbank group companies (Softbank BB and Yahoo Japan). Softbank confirmed that information about 4.6 million customers had been stolen. Company President Masayoshi Son apologised for the breach and promised a 500-yen gift certificate to those customers whose personal data were taken. Police allege that one of those arrested unlawfully accessed the Internet giant’s telephone record database on 11 occasions between November 2003 and January 2004 using the identity and password of a former Softbank employee.

Among measures to improve security, the Ministry of Internal Affairs and Communications is reviewing standards relating to accreditation of designated certification services and making efforts to ensure the safety of electronic signatures and security of certification services. Also, to make it easy for anyone to use strict certification functions using electronic certificates and to enable the safe supply and use of network services, the Ministry from 2004 is implementing research and development on an advanced network certification infrastructure.

In August 2002, the Network System for Basic Resident Registers went into operation, making it possible to have a common national personal identification including name, address, date of birth, gender and residence certificate code. The Basic Resident Register card is issued to those who want one. As well as serving as a public identification certificate, the card can be used in a variety of ways that take advantage of the high-level security functions and information processing functions of IC cards.

In March 2004, the Ministry convened a research group on ubiquitous sensor network technology and has embarked on a four-year "Research and Development for Utilisation of RFID" plan on use of RFIDs in a variety of fields, such as food products, distribution, medical treatment and environment.

2.4.2 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 (Ito et al. 2003).

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.[86]

It's clear from KDDI's product development and that of its competitors that the future ubiquitous network society won't (only) be characterised by invisible computing. In fact, KDDI and others are working on mobile phones that can provide a "multiplexity" (to

[86] See the "Knock! Knock! Ubiquitous" video streaming scenarios at www.kddi.com/english/index.html

coin a word from multiplicity and multiplexing) of services, including e-mail, television, appliance control, location as well as video telephony, Internet access and more.[87]

2.4.3 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 (Ninomiya 2005).

2.4.4 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, of which the following are perhaps the best known.

The **Aoyama-Morikawa Laboratory** (AML)[88] is a research group at the University of Tokyo, the objective of which is to define the architecture, protocols, applications and systems for the future information infrastructure. Its research interests cover ubiquitous networking and its applications, mobile and wireless networking, networked collaboration, and photonic networking. AML is engaged in joint research projects including the Yaoyorozu (aka 8MG) and Ubila projects as well as a New Generation Mobile Network Project supported by the National Institute of Information and Communications Technology (NICT).

The **Hide Tokuda Laboratory** at Keio University is a working group that focuses on operating systems, computer networks, mobile computing and virtual network appliances.[89] It aims to design the future generation of the computing environment. It is engaged in several projects, among which are the following:

[87] www.kddilabs.jp/eng

[88] www.mlab.t.u-tokyo.ac.jp

[89] www.ht.sfc.keio.ac.jp

- UbiLab
- Multimedia and micro Kernel (MKG) Project
- Real-Time Human Device Interaction (RT-HDI) Project
- .HOME Project
- Smart Space Laboratory (SSLab) Project
- A-Project
- Ubiquitous Secure Computing Project
- 21st Century COE Program
- Micro HotSpot Network (MHSN) Project

The **Ubiquitous Computing Laboratory (UbiLab)**[90] develops fundamental and application software. It has created Smart Furniture, which can be placed within an area with no network connectivity so that it becomes a Smart Space, with network connectivity and services. UbiLab members include people from Keio University, Tokyo Denki University and the Tokyo Institute of Technology.

The YRP Ubiquitous Networking Laboratory (**YRP UNL**)[91] was established in 2002 with the aim of achieving a ubiquitous computing environment by embedding micro-computers with communication capabilities, sensors, actuators, etc. in physical objects and having them operate in a concerted manner in processing and exchanging information. The YRP UNL also aims to establish protocols for the next-generation communication infrastructure with the following features:

- real-time communication protocols
- security
- ultra tiny computers
- effortless operation by those without technical knowledge
- human friendly interface including context awareness

[90] www.ubi-lab.org. UbiLab is an undertaking of Keio University and others.

[91] YRP is the abbreviation for Yokosuka telecom Research Park. www.ubin.jp/english/aboutus.html.

- “calm” computing maximising resource savings
- co-operative processing by nodes in the networks.

The laboratory says it especially focuses on building platform systems for ubiquitous computing with good commercial prospects. The director of the YRP UNL is Dr Ken Sakamura, a professor at the University of Tokyo, who among many other things is the director of the TRON Association (see below).

The **Ubiquitous Networking Laboratory** (UNL)[92] focuses on networking technologies ranging from the Internet to small-area wireless networks, including ubiquitous computing and sensor networks. It also studies security issues. UNL is at Tokyo Denki University. Of particular interest to the UNL are sensor networks, protocols and security for ubiquitous computing, home-area networks and network measurement. UNL says that security (confidentiality, authentication and integrity) in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for resource constrained sensor nodes.

The **Distributed and Ubiquitous Computing Laboratory** at Waseda University in Tokyo is researching software for building future digital equipments, such as an information appliances, hardware and new services.[93] The Lab has five groups focused on an operating system for extended information appliances, next-generation human computer interaction, the software component for next-generation mobile devices, sentient artefacts and software methodology on ubiquitous environment.

Privacy issues are also researched. Two staff produced a paper entitled “Privacy-Concern for Context-Aware Environments” (Shoji/Nakajima 2004) which notes that although context-aware computing offers attractive services by collecting information from various sensors, there are dangers for personal privacy since the data retrieved by the sensors may contain privacy information. The authors consider the trade-off between privacy and the quality of services, and present the design of a system under development at the university. Their proposed system controls the trade-off according to a user's requirements, and, they say, guarantees the trustworthiness of the management of privacy information.

[92] The UNL at Tokyo Denki University (www.unl.im.dendai.ac.jp/index.html) should not be confused with the YRP UNL.

[93] http://www.dcl.info.waseda.ac.jp/home/index.html.en

2.4.5 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**[94] 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)[95] 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

[94] www.ubiquitous-forum.jp (in Japanese only)

[95] www.mitf.org

became the TRON Association in 1988.[96] Membership in the TRON Association is open to anyone who shares in the objectives of the TRON Project and agrees to observe the TRON Association's rules.

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. ITRON (=Industrial TRON) is a real-time operating system specification for embedded devices. It is a de facto standard in the Japanese embedded industry and has almost 50 per cent of market share in Japan. It's claimed to be the world's leading such standard. TRON has had mixed success, but ITRON is used in robots, fax machines, digital cameras and many other devices. Prior to the introduction of ITRON, Japanese electronics makers wrote their own operating systems for embedded chips, which resulted in a lot of incompatible software. ITRON addressed this need. It offered specifications for a standard real-time kernel that could be reused for different devices with minor adjustments. According to estimates by the Japanese media, three to four billion microprocessors are running ITRON.

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.[97] 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" (Krikke 2005). The forum collaborates in developing ubiquitous computing solutions using off-the-shelf components. T-Engine enables the distribution of software resources, including middleware developed on T-Kernel, its compact, real-time operating system. The platform also features standardised hardware and tamper-resistant network security. The instigator of T-Engine and its chairman is the ubiquitous Prof. Sakamura (see above). Like the TRON Association, the T-Engine Forum conducts research and development and promotes computer architectures advocated by Prof Sakamura.

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.[98]

[96] www.tron.org

[97] Its website is www.t-engine.org/english

[98] The Chairman of the uID Center is Dr Ken Sakamura. Its website is www.uidcenter.org/english/introduction.html

The uID Center claims to hold the world's most advanced technologies in the fields of small devices and small-sized electronic devices. It is conducting verification tests of the technology in several industries. 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 research and development results of the uID Centre are openly available. The uID Center policy is to authorise all products which meet uID Center specifications and standards.

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. Comprehensive system platforms and solutions for the provision of ubiquitous services are being independently developed by many IT vendors. Such separate developments pose issues concerning user convenience and compatibility among different systems. Thus, the four companies launched their ID Commerce Platform Development Initiative to examine the interface and functional requirements for the ID commerce platform, seek the participation of additional companies, and verify system interoperability. The findings will be broadly disclosed in the future so they may be used by other IT-related enterprises to help prepare the environment for the further development of ubiquitous business and contribute to early realisation of the ubiquitous network society. The companies plan to construct a prototype system and undertake trials in 2005.[99]

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.[100] The specifications will help make advanced mobile devices/applications more secure and help protect against viruses and other threats. The Trusted Mobile Platform specifications were constructed to address security concerns, such as the following: How can data exchanged over the air be protected from eavesdropping? How can the user be certain that information received from a service is authentic and has not been changed since it was created? How is the device protected from malicious downloaded programs such as viruses? The Trusted Mobile Platform will make its specifications open to the public for review.

[99] www.nttdata.co.jp/en/media/2005/042000.html

[100] www.trusted-mobile.org

The **Communications and Information network Association of Japan** (CIAJ)[101] 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.

CIAJ submits proposals and makes industry views and needs known to the government in order to have them reflected in national policies and legislation. Among other activities, CIAJ has set itself these tasks, to:

- collect and analyse information relevant to policy issues, market and technological trends, as well as conduct studies and present proposals;
- promote activities which contribute to widespread and advanced uses of information in socio-economic and cultural activities;
- promote dissemination and advanced uses of network equipment, system solutions, terminal equipment, etc.;
- create guidelines and promote standardisation.

The **Electronic Commerce Promotion Council of Japan** (ECOM)[102] 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 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. The new organisation was scheduled for launch in April 2005. Among the industry members of ECOM are 27 core members including 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. ECOM has had working groups, including the following:

- *Mobile EC WG*

[101] www.ciaj.or.jp/e/index.htm

[102] www.ecom.jp/ecom_e/index.html

The group examines impediments to utilisation of mobile electronic commerce in terms of security and privacy and considers countermeasures.

- *Traceability WG*

The group studies the business models to meet needs of product traceability among industries and methods to manage product-tracking information.

- *EC Site Security WG*

The group researches actual conditions of security measures for electronic commerce sites and helps to enhance security level on sites through study of security technology and new threats.

- *Authentication/Notary WG*

The group examines authentication technologies and considers applicable models. The group considers available modes of e-certificate and analyses attribute information. In addition, the group examines requirements for the long term-storage of e-signed documents, considers actual transactions, and makes recommendations.

ECOM has also been promoting diffusion of IC tag systems and improvement of information sharing among companies. ECOM studies how personal information should be managed, focusing on key points for compliance with the Personal Information Protection Act. ECOM also participates in international discussions for the protection of personal information in electronic commerce. It has supported surveys of technologies for electronic signature and authentication and on security issues in mobile and ubiquitous environments.

2.4.6 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. There have, however, been calls for very large projects (see the aforementioned paper by NRI’s Teruyasu Murakami), but none as yet has materialised. 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 various other documents.

Among the main ubiquitous network society projects are the following:

The **Ubila** project[103], 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 (Kawahara et al. 2004).

The official name of the **Yaoyorozu** project (Aug 2002-Mar 2005)[104] 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.

Keio University’s **21st Century COE** (Centre of Excellence) Programme[105] started in 2002 and is sponsored by the Japanese Ministry of Education, Culture, Sports, Science and Technology. The programme’s research is focused on ubiquitous middleware for smart computing environment and their applications to social issues.

The **Micro Hot Spots** project at Keio University employed “smart furniture”, which can be used to convert non-smart space into a “smart hot-spot”. In other smart room projects, special rooms have had to be specially equipped with sensors and other devices to detect human activity and provide services (Ito et al. 2003).

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

[104] The project’s website is www.8mg.jp/en/outline_goals01.htm. In classical Japanese, the word "Yaoyorozu" (literally "eight million") was used to refer to something that was countless in number, particularly in the phrase "Yaoyorozu no Kami-gami," or "eight million gods." The belief was that gods lived not only in the many old temples throughout Japan, but in the trees and the stones, in the sky and the water, constantly surrounding and protecting us. In similar fashion, the ubiquitous society will have devices and smart computers all around us. The project was given the name “Yaoyorozu” as an expression of hope that these technologies will serve people.

[105] www.coe21.sfc.keio.ac.jp/eng/index.html

The Yokosuka Radio Communications Research Center of the National Institute of Information and Communications Technology (NICT) started a project called the **Next Generation Mobile Network** in April 2002.[106] The target of this project is the development of new technologies to enable seamless and secure integration of various wireless access networks such as 3G and 4G cellular, wireless LAN, Bluetooth, ultra-wideband, fixed wireless access and intelligent transport system. In collaboration with industries and universities, the research centre created a test bed for evaluating new technologies.

The **WISER** project[107] at Tokyo Denki University is focused on development of an ad hoc communication architecture for multiple nodes ("mobile robots") with short-range wireless links for co-operative sensing. The project utilises the movement of nodes as a means of transferring data. The WISER project has applications for disaster areas where it may be difficult to distribute sensor nodes densely (Tobe/Suzuki 2005).

The authors of the **CRUISE/r** project at Tokyo Denki University proposed a ubiquitous personal lost and found system for public transportation passengers using RFIDs, wireless LANs and mobile IPv6. Two factors limit deployment of CRUISE/r. One is the need for co-operation of other people. The other is to avoid malicious messages and spamming. The project recognises the need to consider techniques of filtering undesirable messages. Also, there is a risk that personal information can remain in other people's devices.

2.4.7 Privacy

Of the Japanese projects we looked at, several have taken on board issues of interest to SWAMI. 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 the examination of appropriate policies for handling privacy and clarifying the basic requirements.

Corporate Japan is well aware of the need to be sensitive to the privacy concerns of society. The largest Japanese companies are developing ubiquitous technologies with privacy and security features in mind. While NTT DoCoMo[108] accelerates towards the ubiquitous network society on the back of its i-mode and FOMA offerings, it is sensitive

[106] http://www2.nict.go.jp/mt/b190/e/outline/outline.html

[107] www.unl.im.dendai.ac.jp/wiser

[108] www.nttdocomo.com

to public apprehensions about privacy protection. That concern was driven home in April 2005 when the company issued a public apology for leakage of personal data of DoCoMo mobile phone subscribers who had received discounts following the Mid Niigata Prefecture earthquake in 2004.[109] An employee of a DoCoMo subcontracting company was arrested in April in 2005. DoCoMo said it "takes this incident very seriously and is implementing stringent measures based on Ministry of Internal Affairs and Communications guidelines on the protection of personal data to ensure that such a leak does not occur again." DoCoMo also said it had decided to penalise its president and CEO, a senior executive vice president and an employee who was in charge of the issue. (It didn't say what the penalties were.)

NTT DoCoMo has a 10-point code of ethics posted on its website, point 3 of which says "We respect the human rights of our customers and spare no effort to manage and safeguard their personal information appropriately." Also posted on its website are details of its privacy policy regarding personal information.

KDDI R&D Laboratories[110] says it also places "vigorous" emphasis on security. Its ubiquitous networking R&D is focused on, inter alia, security technology, network attack detection and prevention technology, and privacy protection technology. There are, however, few details about such research on its website (at least, in English).

2.4.8 Identity

Secure means of authentication of identity is an important issue in Japan, as it is in Europe and the United States, and there are projects in Japan which are focused on it. The STONE project, for example, 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 Micro Hot Spots project developed an active authentication system for its smart furniture. The project is currently designing advanced functions such as personalisation and access control, which are important when smart furniture is used in public spaces so that users can discard any personal information.

[109] www.nttdocomo.com/presscenter/pressreleases/press/pressrelease.html?param[no]=546

[110] www.kddilabs.jp/eng/

The Next Generation Mobile Network project at the Yokosuka Radio Communications Research Center is developing and evaluating authentication technology, which can be easily incorporated into terminals and offer high-level security.

2.4.9 Security

As one would expect, the security of networks concerns and affect both the public and private sectors (as well as citizens, of course). Hence, efforts are being made to improve the security of existing and future ubiquitous networks.

The National Institute of Information and Communications Technology (NICT) has established an information security centre, which aims to protect users' privacy, ensure the security of online information, and protect the public from computer viruses. Its research covers techniques and control of ad-hoc networks, cyber attacks and secure protocols to integrate wired and wireless communications.

In order to promote countermeasures relating to violations of information security, the Telecom Information Sharing and Analysis Centre (Telecom-ISAC) Japan was established in July 2002 by three business groups and seven telecommunications carriers.[111] Telecom-ISAC Japan undertakes research and development and has constructed a wide-area monitoring system for the swift detection of incidents. The Ministry of Internal Affairs and Communications has endorsed the Telecom-ISAC Japan initiative and will promote security policies in co-operation and co-ordination with the group.[112]

The MIC itself has set up a Study Group on Platform Functions for the Ubiquitous Network Society,[113] which, among the topics for investigation, is developing measures necessary for ensuring security and safety. The group was expected to issue a report on its work in June 2005.

2.4.10 Trust

So far, in Japan as in the United States and Europe, the notion of trust in ubiquitous computing, ambient intelligence or the ubiquitous network society has mainly been considered in the context of making the networks trustworthy or, perhaps more precisely, of being able to use untrusted networks in a trustworthy way. In Japan, as noted above, there is even a Trusted Mobile Platform, initiated by IBM, Intel and NTT

[111] Japan Telecom, NEC, NTT Communications, KDDI, IIJ, Powered Com and Nifty.

[112] www.oecd.org/dataoecd/25/34/17848902.pdf

[113] www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news050315_3.html

DoCoMo, and its objective is to build on strong security techniques and apply them to hardware and software architectures to create an environment responsive to different trust levels. It is defining a set of protocols enabling device level trust to be extended into the larger network. Undoubtedly, this is all good stuff, but so far, there appears to be little research on the nature of trust, how trust can be earned, how it can be restored once it's been lost, user perceptions of what constitutes trustworthiness and the perceptions of different social groups. These sorts of aspects are important too, especially in view of the u-Japan objective to realise a society in which 80 per cent of Japanese accept ICTs as safe and friendly.

2.4.11 Digital divide

Japan, like Europe and unlike the US, has adopted an explicit policy towards bridging the digital divide in the context of the ubiquitous network society. In fact, bridging the divide is one of the three pillars of its policy. Furthermore, targets have been set for doing so.

The White Paper says Japan must undertake measures to resolve issues including bridging the digital divide. The White Paper says that in order to fully enjoy the advantages of a ubiquitous network society, it is necessary to build a society where everyone, including the elderly and people with disabilities, can freely transmit and access information usually specially adapted information and communications equipment and systems.

The White Paper also notes that the construction of network infrastructure by private companies is not making headway in disadvantaged regions because of such problems as profitability, and the digital divide caused by geographical factors is becoming striking. As a result, policy responses by the central and local governments are called for. The MIC is responding to the regional divide through various projects, including the construction of subscriber fibre-optic networks, the construction and maintenance of transmission towers for mobile telecommunications, and the construction of facilities to ameliorate poor reception of commercial television and radio broadcasting.

In 2003, the Ministry initiated R&D on the network-human interface, covering issues such as a practical multilingual voice automatic translation system for network-connected mobile terminals. In its five-year plan from 2004, the MIC is supporting R&D on such issues as "people-friendly communication technology".

The digital divide issue was raised at the Tokyo Ubiquitous Network Conference in May 2005.[114] In his report, the conference chairman noted that the digital divide is rooted in such factors as geographic, economic, educational and social conditions. To bridge the digital divide towards a ubiquitous network society, an environment has to be established in which the information-disadvantaged, such as the elderly, women, youth, children and people with disabilities can participate equally in socio-economic activities using ICTs, and in which all can enjoy a better quality of life in a secure and reliable environment.

The T-Engine Forum **Autonomous Movement Support project** has already taken steps to this end. It employs various ubiquitous technologies to provide universal services to people suffering from disabilities in Kobe. Demonstrations have targeted the vision-impaired and people in wheelchairs. They have been equipped with a Ubiquitous Communicator with a function to send out an SOS in case of an emergency. Information is provided in several languages (Japanese, English, Chinese and Korean). The demonstrations have also involved local shops and “intelligent” reference points with IC tags attached.

2.4.12 Safeguards

With regard to safeguards, various ideas have been mooted in Japan and they are, not surprisingly, similar to those that have been kicked around in Europe and the US. Among them:

- The use of PKI and biometrics (fingerprints, voice prints, retinas, irises) are assumed for authentication in a 4G environment. Despite some problems with biometrics, it’s assumed that biometrics will become an important source for authentication.
- Software agents that enable individual customers to set their privacy preferences (even dynamically) are also regarded as important.
- Legal structures are necessary and should be strictly applied to network crimes.
- Transparency is important. As noted earlier in this chapter, NTT DoCoMo, like many other companies, has a clear and straight-forward privacy policy which one can read on its website and it has a code of ethics which, inter alia, says it respects

[114] “Toward the realization of a Ubiquitous Network Society”. Chairman’s Report. www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news050517_1.html

its customers' human rights and will spare no effort to safeguard their personal information.

- Media attention and stigmatisation of offenders, even indirect offenders (CEOs who weren't careful enough in supervising what their employees were up to), are salutary.
- Organisational steps need to be taken inside and outside companies, e.g., improving the awareness and knowledge of employees, the formulation of security policies, and regular information security audits.
- Periodic review of applicable standards is a good idea. The Ministry of Internal Affairs and Communications is reviewing the standards relating to the accreditation of designated certification services and is making efforts to ensure the safety of electronic signatures and security relating to certification services.
- Another safeguard is a trustmark. From 2004, the Ministry is carrying out surveys and research with the aim of promoting the establishment of a Contents Safety Mark system so that site operators can indicate the safety of their own sites.

Privacy enhancing technology (PET)

There are several examples of PETs in Japan:

The TRON Association recognises that the future ICT environment needs to be kept safe from unauthorised network access, invasions of privacy, or remote tampering, which requires security guarantees in each of the devices in the ubiquitous network society. One of the TRON security products is T-Dist, a platform that supports distribution of T-Engine-based software. With this platform, middleware is distributed after being encrypted in advance. When executed, the software is decrypted and executed only if a licence controller installed in the loader verifies the licence. When verifying the licence, the use of a secure IC chip called eTRON prevents unauthorised use and allows for secure software licensing management and billing. T-Dist is also compatible with the distribution of applications and content for end-user applications such as games, music and video.

The uID Center provides the infrastructure for managing electronic tags (known as ucodes, short for ubiquitous codes) embedded in or attached to objects. The ucode is a multi-code tag that automatically identifies information stored in bar codes, RFID chips, smart cards and electronic tags. The uID Center assigns unique numbers to each tag and stores data relating to the object in a database held in a server in a distributed network of servers. Information stored on the ucode tags is extracted by a so-called

Ubiquitous Communicator (UC for short), a PDA-like device which can match the code held in a server database.[115] Once the match is made, the UC downloads the relevant data from the server. Public key encryption technology is used to ensure secure communications. The uID Center operates its own certification authority for secure communications.

With ubiquitous embedded objects, the uID Center recognises the possibility that automatically identified personal information might be leaked out and misused. To prevent this from happening, the uID Centre says it is putting "the utmost effort" into developing technologies that protect security and privacy. Specifically, the uID system is protected by eTRON (Economy and Entity TRON), a wide-area distribution system architecture based on tamper-resistant hardware. eTRON chips are installed in T-Engine boards to prevent tapping and falsification; it also ensures that electronic information is safely delivered through insecure network channels, including the Internet. eTRON has a flexible cryptographic architecture and an ID protection protocol to prevent third parties from tracking the tag owner's activities.

Legal and regulatory safeguards

As countermeasures against illegal and harmful contents, the Ministry of Internal Affairs and Communications is providing assistance to business groups on the formulation of related guidelines and conducting a publicity campaign so that the "Law on Restrictions on the Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identity Information of the Sender" (the so-called the Law Concerning the Liability of Internet Service Providers) can be properly enforced.

The Unauthorised Computer Access Law enacted in 2000 prohibits unauthorised access either by using a person's ID and password without authorisation or by attacking a security hole.

The Telecommunications Business Law was revised during the 156th session of the Diet to newly establish accountability. The amendment stipulates that a carrier or agent must explain the content to the consumer at the time of concluding a contract and that a carrier must accurately and promptly deal with any complaint or inquiry from a consumer.

To deal with the problem of spam, Japan has adopted a "Law on Regulation of Transmission of Specified Electronic Mail". The MIC is promoting voluntary responses

[115] See www.ubin.jp/press/pdf/TEP040915-u01e.pdf for a description of the functionalities of the Ubiquitous Communicator, among which is a biometric for fingerprint authentication.

by carriers and increased awareness among users. The government submitted an amendment to the Anti-spam Law to the Diet in March 2005 which extends the target of e-mails covered by the law to include e-mails sent to business-use addresses in addition to private-use addresses. The amendments expand the scope of prohibition against sending spam e-mails and introduce direct penalties to malicious spammers.[116]

In May 2003, the government promulgated the Law Concerning the Protection of Personal Information (Law No. 57, 2003), which came into effect on April Fool's Day 2005. The law applies to any company with offices in Japan that holds personal data on 5,000 or more individuals, including company employees. Personal data as defined by the law includes a person's name, address, date of birth, sex, home and/or mobile phone numbers and e-mail address if that address is recognisably the person's name. The new law requires a new regulatory infrastructure for protection of personal information by businesses and the government. Each ministry is required to produce guidelines to cover the industries over which they have jurisdiction. The MIC has set information management guidelines for the telecommunications industry and the broadcasting industry.

The law stipulates five basic principles regarding the collection and use of personal information: Information must not be used other than for clear, specified purposes; information must be collected properly; information must be always correct and up-to-date; information must be kept secure and safe from leakage; and information must be handled in a transparent manner that properly involves individuals. These principles apply to all businesses and organisations that deal with personal information.

The law defines a set of regulations governing how private businesses may make use of personal information. Businesses must make clear to the individual the intended use of such information; not pass on the information to a third party without the prior consent of the individual; upon request by the individual, release the information, correct mistaken information, or discontinue use of the information; and supervise employees to make sure the information is not used improperly. Companies are

[116] Industry has also taken up the fight against spamming. Recognising that spam e-mail is a serious problem that requires a concerted, industry-wide effort to resolve, Internet Initiative Japan, KDDI, NTT DoCoMo, Panasonic Network Services, Plala Networks, Vodafone K.K., Japan's major Internet service providers (ISPs) and mobile telecommunication carriers established the Japan E-mail Anti-Abuse Group (JEAG) to examine and implement technological countermeasures against e-mail abuse. About 30 companies make up the founding members of JEAG. See www.nttdocomo.com/presscenter/pressreleases/press/pressrelease.html?param[no]=539

allowed to pass on information to a third party if they have notified the individual in advance that the information will be shared unless the individual requests otherwise or if sharing such information has a legal basis. Failure to comply with administrative recommendations or orders may result in a maximum prison sentence of six months or a fine of up to 300,000 yen. The law does not, however, explicitly prohibit the transfer of information to other countries not having similar privacy laws.

Guidelines

Perhaps the most important guidelines for protecting privacy will come from the Ubiquitous Network Society Charter proposed by a working group of the Policy Roundtable for Realizing Ubiquitous Network Society. The charter brings together the basic principles and shared perceptions for a ubiquitous network society.[117] The charter strikes a balance between free and diverse information distribution, and safe and secure information distribution. In the context of the latter are privacy, information security, intellectual property rights and information ethics. The Ministry of Internal Affairs and Communications invited comments, in Japanese, concerning this draft from 18 January until 18 February 2005.

[117] "MIC invites comments concerning Ubiquitous Network Society Charter (draft)". Press release. 18 Jan 2005. www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news050118_1.html

3 Analysis of ambient intelligence scenarios

3.1 Introduction

This chapter presents an analysis of the vision of a future in which ambient intelligence technologies are used in everyday life from the point of view of privacy and social implications. For this analysis, the vision was constructed based on a review of more than 60 project and roadmap scenarios and research publications with the goal of understanding where the joint efforts of numerous AmI researchers lead and how they are going to change our lives. The vision of a future everyday life is a mixture of many diverse applications ranging from relatively-easy-to-realise working research prototypes to scenarios in the distant future taken from roadmaps. The many aspects of our everyday lives have been clustered in the following application domains: home, work, learning, health, shopping and mobility.

The structure of the paper is the following: first, we present views of several researchers on privacy and its aspects. We then explain how we synthesised the AmI vision from numerous papers and which aspects (dimensions) of scenarios we consider as important for our analysis. Next, we present the main application domains and their future visions, as well as their specifics. After that, we list the main benefits and threats identified in the scenarios and open issues, and we present our conclusions.

3.2 Aspects of privacy

Bohn et al. (2005) present a good overview of different aspects of privacy, partially as a summary of a previous research. First, they present different aspects of privacy:

- *Privacy as empowerment.* Seeing privacy mainly as informational privacy, its aim is to give people the power to control the publication and distribution of information about themselves.
- *Privacy as utility*. From the viewpoint of the person involved, privacy can be seen as a utility providing more or less effective protection against nuisances such as unsolicited phone calls or e-mails. This view follows a definition of privacy as “the right to be left alone,” where the focus is on minimising the amount of disturbance for the individual.
- *Privacy as dignity.* Dignity not only entails being free from unsubstantiated suspicion (for example, being the target of a wire tap, where the intrusion is usually not directly perceived as a disturbance), but also focuses on the equilibrium of

information available between two people: as in a situation where you are having a conversation with a fully dressed person when you yourself are naked, any relationship where there is a significant information imbalance will make it much more difficult for those with less information about the other to keep their composure.

- *Privacy as a regulating agent.* Privacy laws and moral norms can be seen as a tool for keeping checks and balances on the powers of a decision-making elite. By limiting information gathering of a certain type, crimes or moral norms pertaining to that type of information cannot be effectively controlled.

Second, they describe what people perceive as borders protecting their privacy:

- *Natural borders.* Physical borders of observability, such as walls and doors, clothing, darkness, and sealed letters and phone conversations. Even facial expressions can represent a natural border against the true feelings of a person.

- *Social borders.* Expectations with regard to confidentiality in certain social groups, such as family members, doctors and lawyers. This also includes the expectation that your colleagues do not read personal fax messages addressed to you, or material that you leave lying around the photocopier.

- *Spatial or temporal borders.* The expectation by people that parts of their lives can exist in isolation from other parts, both temporally and spatially. For example, a previous wild adolescent phase should not have a lasting influence on the current life of a father of four, nor should an evening with friends in a bar influence his coexistence with work colleagues.

- *Borders due to ephemeral or transitory effects.* This describes what is best known as a “fleeting moment,” a spontaneous utterance or action that we hope will soon be forgotten, or old pictures and letters that we put out in our trash. Seeing audio or video recordings of such events subsequently, or observing someone sifting through our trash, would violate our expectations of being able to have information simply pass away unnoticed or forgotten.

Other works give more insight into privacy aspects. For example, Nissenbaum (2004) presents a model of informational privacy in terms of contextual integrity, namely, that determining privacy threats needs to take into account the nature of a situation or context: what is appropriate in one context can be a violation of privacy in another context.

Nissenbaum also describes the connection between privacy and autonomy: the freedom from scrutiny and relative insularity are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide freedom for people to formulate for themselves the reasons behind their choices, preferences and commitments. Thus, the privacy aspect called "utility", the right to be left alone, is much more than just a utility because it is extremely important for personal development.

Singer (2001) argues that privacy is not only about disclosure of dangerous information or disturbing a person at a wrong time or with information on a wrong topic. For example, personalisation of advertisements may seem to be beneficial. Instead of a bunch of useless and time-robbing advertisements about, e.g., new skis, a client who is not interested in skiing will receive advertisements about what he is truly interested in, for instance, new fishing rods. However, such personalised or targeted advertising is not so innocent or beneficial in a long term because advertising views people as bundles of desires to buy more and more, and this view is partially true. Precise advertisements are harmful because they proceed to reshape human nature to fit the picture of "being a bundle of desires", diminishing people's capacities of reasoned choice and thoughtful action. Thus, Singer’s work also links privacy to personal development.

3.3 Constructing scenarios – Objectives and the specific focus/ purpose

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 (good examples are the ISTAG scenarios (IST Advisory Group, 2001)) or scenarios developed by projects aiming at presentation of 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 can be found in research publications. These scenarios usually concentrate on a certain functionality of a system prototype described in the publication, and the storyline in these scenarios

is detailed only in parts which describe the system functionality. Some research publications describe the results of a prototype evaluation which can help in understanding AmI implications.

- 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, for example:

> "There is an on-going trend towards out of bound (off-piste) skiing. Accordingly, the number of alpine recreationists in backcountry terrain, such as skiers, snowboarders, ice-climbers, etc., has increased in the last years. At the same time recreationists go beyond their limits, underestimate the danger of avalanches and risk their lives without the appropriate awareness of avalanche risks. Statistical analysis of avalanche accidents during the last 30 years has revealed that successful avalanche rescue has to aim at rescuing victims within the first 15 min. Avalanche survival chances rapidly decrease with time and after 15 min there is the biggest decline from 90% to 30%. It is noteworthy that three quarters of all avalanche victims die from asphyxiation, only one quarter is killed from trauma." (Michahelles 2003)

This description is about sports activities in mountains and technology helping to save lives of avalanche victims, but it is not presented as a storyline. However, such descriptions often suggest interesting application areas which one may not find in more elaborated scenarios of the first or second types, and it would be a mistake to miss such new application areas; moreover they are not pure visions, they are working prototypes. One can depict the role of scenarios as follows:

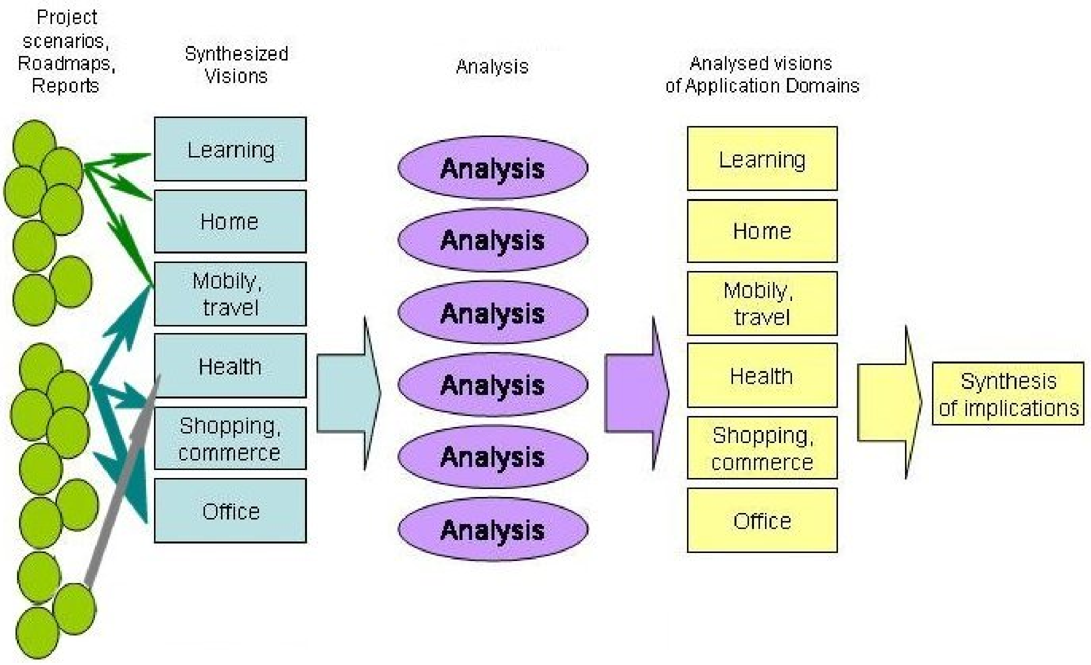

Figure 1: Analytical Framework

The SWAMI partners have synthesised future visions from the material we reviewed. The 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. A more detailed analysis than that presented here in summary form can be found in the Annexes of the deliverable.

The most elaborated scenarios which we used for the creation of the future vision were, first, the well-known ISTAG scenarios for Ambient Intelligence in 2010 (IST Advisory Group, 2001). These are four scenarios describing mainly travelling, shopping, learning and communications in the future. Second, the ITEA Technology Roadmap for Software-Intensive Systems (ITEA 2004) has presented several screenplays describing a family holiday trip (sightseeing and solving health and work problems during the trip); travelling for work and communications with family members; and project work in future. Third, elaborated scenarios were built by AMSD project (AMSD 2003) (these scenarios mainly describe work and driving in the future); by the COCONET project (Aschomeit/Höbig 2002) (four scenarios describing different work aspects in a future), by the MIMOSA (Kaasinen et al. 2005) and Smart-Its (Gellersen 2002) projects which describe what kinds of opportunities open in everyday life, e.g., in sports, health, shopping and work when everyday objects are augmented by communication and reasoning capabilities; by the 2WEAR project (Savidis 2001; also augmentation and connections of everyday objects and usage of AmI in many aspects, e.g., work, travel, health and communications between people; by the Amigo project[118] (home environment); by the CANDELA (Sachinopoulou 2005) and MiMe[119] projects (scenarios describing life cycle of home media).

Such projects as InterLiving[120], ACCORD (Åkesson 2001), RUNES[121] and Oresteja (Palmas 2001) have presented short scenarios: InterLiving project scenarios of communications between family members and other people inside and outside the home; ACCORD and RUNES project scenarios of usage of augmented artefacts in home, work and health domains; Oresteja project scenarios of using physiological sensors in evaluation of the user's reactions to everyday events, e.g., in learning and phone conversations.

Most other components of future visions were taken from diverse research publications and projects' goals. We consider all elaborated scenarios, short scenarios, research publications and projects' goals equally important for the construction of visions because all of them present novel ideas and interesting functionalities of ambient intelligence in the future world.

While synthesising visions from numerous sources, 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;

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

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

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

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

- 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 level of AmI, first, makes it easier 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 Deliverable 1.1 (Masera 2003), 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.

3.4 Future visions

3.4.1 Home application domain

Home, being the most private place for people, 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, and it is difficult to say what information about someone can not be found in the home environment. Second, people perceive their homes as a place where they can be free from intrusion, relax and think in peace, i.e., "to be left alone". As Nissenbaum said (Nissenbaum 2005), this privacy aspect is very important for personal development.

Many AmI projects and roadmap scenarios are targeted at supporting the home environment in the following ways:

- communications between people, both between house inhabitants and between people inside and outside the house: exchanging plans and location information or just chatting, sharing intimate media, welcoming guests or preventing robbery. 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 capabilities present in future homes are mainly aiming at building 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;
- giving reminders of all kinds 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 assessment of the physiological state of people during conversations, especially phone calls);
- helping in finding of personal belongings, e.g., toys or lost keys;
- controlling diverse home appliances (from lights, fridges and washing machines to automatic doors with access control) and numerous household objects (including clothes, keys and food products) for making household duties and maintenance tasks easier, and for making possible remote access to home;
- increasing safety and security by tracking people, appliances and objects; preventing or fast reporting of accidents; handling access control;
- entertainment (summarising TV programs, gaming and so on) and increasing comfort levels;
- functionalities from health and shopping domains, to be discussed in the next sections.

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 supporting infrastructure is assumed to be present everywhere.

Home is a private sphere which can become semi-public when visitors arrive. However, with the trend to increase connectivity between home inhabitants inside and outside home space and to increase connectivity between home and other spaces, such as organisations and homes of other people, there is a danger that home space becomes less private space 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 feel 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 communicational and even computational 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 level at home.

3.4.2 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 capable of investing more money than ordinary people in their homes. 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.

AmI projects and roadmap scenarios target supporting the future work environment in the following ways:

- communications between people, both between people in the office and between people inside and outside the office environment; both work-related and non-work-related communications. 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 the working problems. 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.

3.4.3 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;
- cure of diseases, which is directed towards short-term recovery. Cure starts from diagnosis (by video link and so-called "lab on 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 crisis 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, with the goal of supporting autonomous or semi-autonomous life and making the caretaking process easier. The means to achieve this goal are, first, embedded intelligence capable of tracking activities, detecting anomalies and giving advice inoffensively and, second, 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 the treatment;

- supporting 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 the help of sophisticated embedded sensors and/or actuators tracking the user's actions and health continuously.

3.4.4 Shopping application domain

Ambient intelligence applications in shopping and commerce aim at creating a user-friendly, efficient and distributed service support to the customer, such as managing the search for and selection of merchandisers by the customer, 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 supports the customer to compile 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, which are collected by profiling customers;
- the AmI-enabled store lets shoppers at the site find and select items for purchase by using intelligent tags for goods and by intelligent terminal devices for the customers (shopping cart, mobile personal device) 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 processing, 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 any time. Scenarios which describe shopping by someone's physically visiting shops don't specify shops' locations, thus implying that shops can be found everywhere. Scenarios of "order and delivery" imply presence of a delivery infrastructure, which is more likely to be developed first in urban areas, although scenarios don't mention it explicitly.

3.4.5 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, central not only to competitiveness and employability but also to social inclusion, active citizenship and personal development. 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., learning on purpose 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 distant future "Annette and Solomon" scenario from ISTAG;
- informal learning, i.e., learning 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.

3.4.6 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.

3.5 Observations about AmI visions

We consider the following dimensions as important for scenario analysis from the point of view of privacy threats and social implications: first, activity supported by AmI and the environment where the scenario takes place. These dimensions are crucial in any application domain, as is evident from the preceding section. In this section, we analyse other dimensions of the scenarios.

3.5.1 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 an individual activity of a healthy adult (in shopping scenarios, an individual can have an allergy).

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. In scenarios describing how a user is woken up by cheerful music, the user is either assumed to be sleeping alone or that all family members wake up at the same time and by the same music, which is not always desirable. Similarly, shopping scenarios often neglect the fact that shopping is not an individual but rather a group activity, where family members often have very different responsibilities and decision rights. It is seldom analysed that children may have the right to put certain things on a shopping list, but that parents need to be notified and given the right to veto this decision. 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 or to collect right things. They are rarely presented as active human beings with their own responsibilities.

Significant effort 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 or notification service in order to check what their children are doing, and it is not clear whether the children have rights to avoid being observed by parents at any time. Children are described as activating communications with adults mainly when adults are travelling.

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 are the scenarios of the MIMOSA project (Kaasinen et al. 2004) where AmI advice is not presented as always perfect and the possibility of misunderstandings with the AmI system is considered (see Figure 2 below).

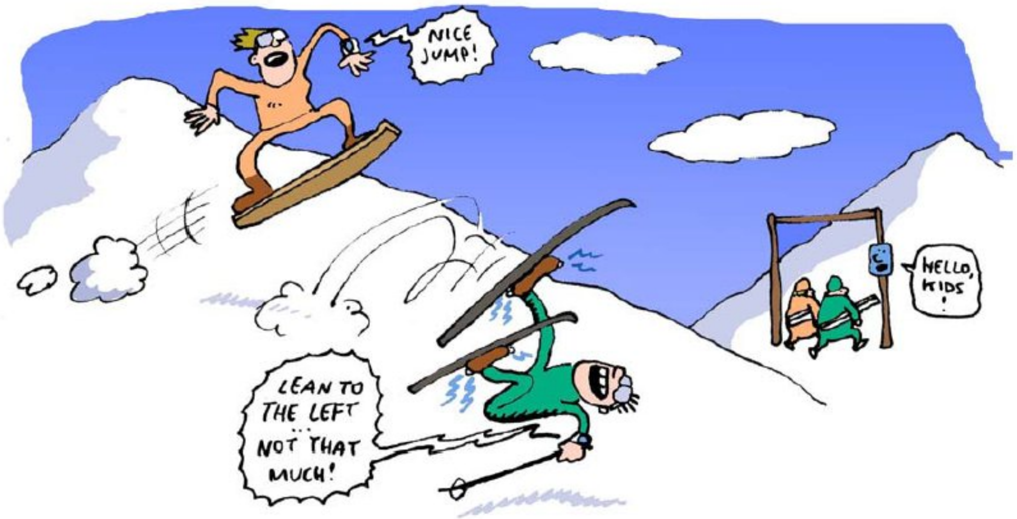

Figure 2: MIMOSA Downhill Skiing Scenario (Source: Kaasinen et al. 2004, p. 12)

Another general rule is that 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) assume that all people have accepted the new technologies.

3.5.2 AmI control level vs. person control level

We suggest distinguishing 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 high level 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 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 with them.

An important feature of AmI with high level 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 (Palmas et al. 2001), 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.

In some scenarios, AmI controls phone communications; it makes decisions about whether to connect a user with the calling person (often a family member) or not. In the ISTAG "Dimitrios" scenario, this AmI functionality is presented clearly: the personal device assistant can even mimic its owner's speech and talk to callers on his behalf. In scenarios which describe "always on" video connection between two locations, it is usually an AmI task to close the connection if predefined rules state that it is not desirable or needed anymore, or if it detects a privacy threatening situation.

In the work domain, AmI is broadly applied to working tools (simulators and documentation), and in this sense, it has a high-level control over the work because an individual's decisions are based on simulation results and automated recordings of meetings. Although AmI just presents simulation results, and the decision is left to a person, it raises a question about how well simulators can take into account complex real-world systems and predict different usage situations, and whether people will rely too much on simulators instead of using their own imagination and creativity.

3.5.3 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 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 which require high security (like immigration control, or protection of professional secrets, or access to health data) and which 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 very 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 location of a car which has been 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, is also known to AmI systems in work and home environments.

Intimate and sensitive data such as health information is 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. First, personal/wearable devices have to communicate with systems in the physician’s surgery and in the hospital. During this ad hoc communication, the most sensitive information (identity, health history, etc.) is exchanged. Second, mobile emergency systems use ad hoc communication with third party nodes as relays for data transmission, e.g., in the 2WEAR scenario (Savidis et al. 2001); the communication devices of other cars and a gas station are used to transmit an emergency call that includes sensitive information about the identity of the injured person. 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. This information includes user profiles created from the collected data about shopping behaviour; travel preferences; user profiles created from web surfing, watching TV; and from e-learning exercises. Such data can reveal a lot about a person's psychology, lifestyle, finances, health and intelligence.

Professional skills (usually stored in a central database) may not be regarded as very sensitive data, but they could be of high interest to terrorists searching for a chemist or computer specialist. Although such data are less sensitive than a person's identity data, they are of high interest to many more people and organisations because the data have a commercial value, and because one does not need to be a criminal in order to benefit from collecting such data. It is also worth noting that 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.

Probably the least sensitive information presented in the scenarios is information about the infrastructure of smart spaces, locations of objects and ways to control the smart space remotely. However, this information may be useful to criminals for robbery or acts of terrorism. For example, when people leave home, they take their personal device assistants with them, and these assistants carry a lot of information about homes and people and provide easy remote access to home. This leaves a lot of possibilities to a malicious hacker to initiate arson or gas leakage remotely.

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. Probably the home, as the most private environment where people feel most secure, and a personal device assistant, which is always with a person, have the most data about people's identities, personalities, health and finances. This creates a high risk when a personal device is lost or stolen.

3.6 Enabling Technology

3.6.1 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.

In this paper, we have reviewed many existing ambient intelligence scenarios from roadmaps and project applications, and although the total number of projects and scenarios is so large that it is impossible to review all of them, we believe that we have achieved a good overall understanding of research activities in AmI. Since roadmaps and ongoing projects determine our future, we will summarise below our findings about enabling technologies as they are currently being developed, their importance for realisation of the vision and their threats to privacy.

Ubiquitous computing systems can not 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.

3.6.2 Ubiquitous communications

After reviewing numerous scenarios, we have come to the conclusion that almost all of them require ubiquitous communications to be realised, 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 actually their convergence into all-IP all over the world. (Alahuhta 2004). 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 (Bruce Schneier, described by *The Economist* as a "security guru," 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 (Schneier 1999)).

At least the two first 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 Wireless Security Center of Excellence (Whitehouse 2002), recommends to increase security of GPRS networks (used currently for Internet access by mobile phones) 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, either at the very moment of communications or possibly later, the ability to link the data to the user identity; second, communications which don't require such linkage. Communications of the first type might require linking of data to the real identity of users for different reasons, very often for 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. However, there is no need to find a seller if the buyer is satisfied with the deal. Thus, in communications of the first type, the main goal is to hide the user's identity from everybody except for 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 since devices become increasingly personal, 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. One suggested application is attaching RFID tags to personal belongings for making household tasks computer-supported. For example, RFID tags can help to find lost keys or eye-glasses (Orr 1999). Other suggested applications are usage of RFID tags in e-passports (Juels 2005), credit cards and generally everywhere (Ward 2004).

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 (Knospe 2004). 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.

3.6.3 User-friendly interfaces

AmI scenarios describe highly advanced user-friendly interfaces, most popular of which are speech interfaces capable of understanding of a person’s natural speech (that is, the users are not restricted by a set of commands and can use any words and phrases when 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/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 being used; on what the system is doing with the user data after they have been input (how does it process, store or transmit them?); and whether the interface is to a public or personal device.

Due to small screens of personal devices, 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.

3.6.4 Embedded intelligence

An incomplete list of embedded intelligence (by "embedded intelligence", we mean the part of ambient intelligence which performs reasoning) functions 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.

First of all, 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 (2004) has proposed that sensitive patterns in data mining be detected automatically and treated cautiously.

Second, 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 reasonably expect a user to memorize" (Schneier 2004), 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 PIN code or touch a fingerprint sensor?

This leads to the fact that 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.

Third, with the increased autonomy of computer devices of all kinds, the security of contents residing there becomes a major issue. For example, one of the main tasks of embedded intelligence in most AmI visions 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, i.e., attempts to obtain a user's passwords by sending a fake e-mail from a user's bank which prompts the user to click on a provided link and enter his password on a fake web page which looks like the real web page of the bank. 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.

3.6.5 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, i.e., using somebody else’s biometric data for one’s own purposes. 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 can not be stolen, for example, in the form of encrypted templates which would prevent restoration of raw data. Yet another problem is interoperability between different biometrics systems around the world, 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.

3.6.6 Summary of enabling technology

We have listed the main enabling technologies needed for implementation of the AmI vision, and privacy threats arising from information losses which are possible with current technologies. Privacy threats and those associated with long-term AmI usage will be analysed in more detail below.

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.

3.7 Threats in a world of ambient intelligence

Privacy, identity, security and trust are central issues in ubiquitous computing visions and have been identified as such from their earliest inception (Weiser 1993). Many in the research and development community clearly recognise the inherent challenge that an invisible, intuitive and pervasive system of networked computers holds for current social norms and values concerning privacy and surveillance.

The inherent privacy challenge from ubiquitous computing stems from two innovations necessary to its success: the enhanced ability to collect data on people's everyday interactions (in multiple modalities and over large spans of time and space) and an enhanced ability to quickly search large databases of that collected data, creating greater possibilities for personal profiling, and other forms of data mining (Bohn et al. 2005). One leading researcher in the field has identified a set of generic privacy concerns that ubiquitous networks will very likely raise for users (Ackerman 2004):

- A pervasive network of interconnected devices and communications will mean that the sheer quantity of personal information in circulation will increase greatly.
- The introduction of perceptual and biometric interfaces for certain applications will transform the qualitative nature of personal information in circulation.
- In order to offer personalised services, ubiquitous networks will require the tracking and collection of significant portions of users' everyday activities.

If users are to be persuaded to participate in a ubiquitous network society, then they will need to be given assurance that their privacy will be protected at all times. The challenge is daunting if we consider the privacy concerns and mistrust that have followed from the introduction of RFID tags and smart cards into the marketplace. For instance, the American pressure group CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) has been lobbying against the use of RIFD tags in consumer products, publishing an ominous warning on the website spychips.com:

> "Unlike a bar code, these chips **can be read from a distance, right through your clothes, wallet, backpack or purse** – without your knowledge or consent – by anybody with the right reader device. In a way, it gives strangers x-ray vision powers to spy on you, to identify both you and the things you're wearing and carrying."[122]

The rhetoric of such 'x-ray vision' and corporate conspiracy that is sprinkled throughout many critics' websites and publications could be criticised for being alarmist and even inaccurate with respect to the limits of current RFID technology, but given that these very early steps toward a ubiquitous network society have the ability to create such a furor, what might be in store for the far more ambitious undertakings proposed by the visionaries?

Almost all analysed scenarios postulate or assume benefits of ambient intelligence while only a minority refer to the threats associated with AmI. In almost all cases, there is a delicate balance between the benefits and threats because for many applications it is necessary that data are collected from the user, processed and matched with other information. A few types of threats are evident from the scenarios – either explicitly or implicitly.

In general, people tend to accept new technologies without worrying much about privacy if they get sufficient benefits from them (e.g., use of mobile phones and GPS in spite of the risk of location tracking). Nevertheless, it is fair to assume that risks to privacy will be increasing inevitably in the AmI world and, consequently, privacy protection should be built into AmI systems rather than relying on user control over personal data. While one should assume a certain awareness by users about information flows ("Who is responsible for my data and where are my data stored?") and that control over those flows is needed, there is, at the same time, a belief that control should not impose an unacceptable burden on the individual (Winters 2004).

To complicate the situation even more, privacy and ethics are person-dependant, culture-dependent and situation-dependent. Thus, the big challenge in a future world of ambient intelligence will be not to harm this diversity, which is at the core of an open society.

3.7.1 Surveillance of users

The availability of data about virtually every citizen can provoke the desire of governments to access the data for the common welfare as in law enforcement and the fight against terrorism. Other institutions responsible for health insurance may justify

[122] http://www.spychips.com/what-is-rfid.html (accessed 19 May 2005).

their actions on similar grounds (even when their actions are unlawful or at least questionable). Since AmI applications are envisaged to be implemented in many spheres of life – even those where privacy has been considered sacrosanct such as in the home – it should come as no surprise that some critics raise the spectre of an Orwellian police state.

Apart from this, the prospect and realisation of increasing surveillance can have very concrete consequences for the citizen: The disclosure of health details, personal preferences, habits and lifestyle to an insurance company or to an employer can easily lead to discrimination (higher insurance contributions, reduced career prospects, even denial of insurance coverage and job layoff), blackmailing and problems in human relations.

The possibility of a retailer's being able to monitor the shopping behaviour of customers can not only lead to an optimised supply chain, it is also the basis of the "transparent customer" who can be manipulated and controlled. Market transparency due to more information as envisioned by most proponents of the AmI world of shopping may be foiled by the effects on the supply side like favourable purchase conditions only for selected groups while others might be disadvantaged or even excluded from the benefits of AmI shopping.

Some of the scenarios argue that it is useful for the user to know if an acquaintance is in his vicinity. Maybe so, but the downside is that disclosure of a person's position can not only threaten his privacy but also facilitate terrorist attacks, robbery or kidnapping.

Even seemingly useful and simple surveillance of the elderly intended to improve care may harm their dignity: Researchers have proposed an "intelligent bed" that tracks the weight of the user. While it is possible to detect abnormal loss of weight, it can also be used to determine when residents get into or leave their beds, if they are having a quiet sleep, or indeed how many people are sleeping in the bed. All of these unintended uses are highly undesirable (Beckwith 2003).

3.7.2 Identity theft

Identity theft is the act of obtaining identity information without the concerned person's consent and for future activities criminal or not (intent). The more widely personal information becomes available, the greater is the risk of its being stolen by malicious persons and being used for fraud and other illegal activities. Here one has to distinguish between the local storage of key personal information on a personal mobile device (like a PDA or wearable computer) and the storage of personal information on one or more remote servers. The personal device is at risk of being stolen by a malicious person and could then easily be used. Personal data on a remote server may be better protected; the damage, however, may be much bigger, once an intruder has cracked the protection. If the information is stored on multiple servers operated by different providers, this risk grows. Once a malicious person has succeeded in stealing personal identity data, he is in the position to spy on any activity of his victims, use it for any kind of fraud, use it for terrorist attacks and even harm the life and health of his victims.

It is not necessary to steal identity information in a physical way, a copy alone is useful. In addition, it is not necessary to use information in a physical way either. Indeed, identity fraud can be perpetrated anonymously (making a purchase by telephone or by Internet). In contrast to the past, a buyer no longer needs to be physically present at the point of purchase, making fraud easier to carry out and reducing the risk of being caught for the identity thief.

The methods employed to steal identity information can be offline and online. Offline methods group the theft of the wallet, the purse, the theft of information by rummaging a home or car, by examining private mail after diverting or stealing it, by a phone call with a bogus premise, by a fake survey, and so on. Online methods encompass attacks on computers, online accounts, PDAs, etc., interception of financial transactions, fictitious websites that ask for personal information, phishing emails, etc. The list of means is continuously evolving as new technologies emerge and new vulnerabilities are exploited.[123]

In general, a person is unaware of the identity theft especially in cases of online methods and sometimes this same person ignores the reuse of his identity for impersonation purposes. How does a person discover whether he is a victim of identity theft? In case of involving a stolen wallet or purse or information in your home or car, theft is obvious but in other cases the discovery comes later, by monitoring bank accounts, by company notification, by refusal of a loan application, etc.

3.7.3 Malicious attacks

An attack can be active or passive. An active attack is a deliberate alteration or destruction of data in a message or creation of false data. A passive attack consists of unauthorised monitoring, but not alteration or destruction of data (e.g., wiretapping).

[123] Bluesnarfing, for example, exploits new vulnerabilities which arise when mobile phones are coupled to Bluetooth technology. Here, an attacker could read, modify or copy the agenda and all kinds of personal data without leaving any traces of intrusion. http://www.phonecontent.com/bm/news/nokia/360.shtml

The purpose is to acquire the information. A passive attack occurs when someone listens to or eavesdrops on network traffic

Complex systems like the ones described in many scenarios can become a target of malicious attacks (viruses, denial of service). Disruption to the operation of an AmI network may result in a loss of convenience as a minimum and/or severe damage ranging from financial loss to death:

- Sabotage of AmI systems can have a wide variety of consequences with the open question about who is or should be legally responsible for AmI failures and the consequences thereof.
- The misuse or manipulation of home applications might result in arson.
- The malfunction of healthcare and emergency systems can be a risk for the life and health of the affected persons.
- Businesses based on AmI can be ruined when the system is put out of operation or if a malicious person or competitor manipulates his back office system.
- Since AmI applications will become pervasive in many spheres of life, citizens and businesses will become increasingly dependent on the availability and dependability of the system. An attack at the right place of the AmI infrastructure may cause a temporal breakdown of activities in business and society, so system diagnostics and deployment of fallback mechanisms are needed.

3.7.4 Digital divide

The pervasiveness of ambient intelligence applications in almost every sphere of life poses the threat of social pressure and digital divide.

People may be forced to use AmI technology. This may be direct as in the case of (health) insurance companies that only give insurance protection when their clients are using some kind of health monitoring system. Or the pressure may be indirect, since most day-to-day activities involve the use of AmI and only leave the choice to use the system or to abandon the activity. Even if a person accepts to use AmI applications, he will be bound to routines predefined by the system. This will limit personal freedom and self-determination. Unavailability of the system for non-routine tasks or incorrect responses might harm individual development at the personal, social and/or professional levels.

Relying on remote communications and automated health care decreases personal communications, which can lead to isolation and feeling lonely, especially in elderly people. It can create difficulties in finding friends or developing trust. Moreover, if children spend too much time in virtual worlds, they may not be well enough prepared for the challenges of real life; they may be irresponsible, unable to communicate with other people or unable to be alone.

Since many functions in everyday life will become dependent on AmI systems, people may be hindered in their personal development and lose the ability to manage their lives. This can result in a lack of self-confidence and personal depression.

AmI personalisation capabilities can lead to conflicts between group and/or family members, when interests are different, but AmI adapts to only one person. Many of the scenarios do not take into account the fact that people are not only individuals but also members of a wide variety of social groups.

AmI applications and services will probably not be free of charge with the result that not all citizens will enjoy all of the benefits that AmI will offer – even in fields that have been regarded as a public utility. This is especially grave in the field of education where society could be divided more sharply into well-educated and less well-educated people.

The deployment of AmI finally challenges the relationship between different actors. For example, AmI gives parents very powerful means to control their children, but it raises the question from which age a child's privacy should be respected, and who sets the limits: government or the family?

3.7.5 Spamming

Profiles of individuals built from data collected through use of AmI technologies can be used for spamming those individuals with more or less useful but in most cases unwanted information.

The availability of personal information is at the very heart of personalised services, but such information can be used for any kind of spamming. The example of the Internet has shown that this effect can hardly be stopped when there are few effective rules or explicit mechanisms for the individual to control where his personal data are stored and for which purpose they may be used or passed on.

Personalised information may be useful, however, when a certain threshold is exceeded even wanted and useful information may lose its value because the user is no longer able to assimilate and make use of the information (information overload).

4 Existing legal framework for AmI

4.1 Preliminary remarks

This overview of the existing legal framework for Ambient Intelligence (AmI) is not an attempt to make an exhaustive analysis of all possibly applicable laws. The aim is rather to provide a wide overview of relevant laws in relation with AmI.

We tackle seven subject matters: (1) privacy and data protection, (2) e-commerce and consumer protection, (3) torts and liability, (4) intellectual property law, (5) ICT law, (6) criminal law and (7) jurisdiction and applicable law. For each subject matter, we describe and summarise the applicable law and we try to identify possible AmI-related problems and challenges in regard to privacy, identity and security.

We study the legal aspects of AmI from a European Union perspective. Consequently, we mainly focus on European Union legislation and we only describe international legislation which is relevant for European policies. Although the European Union is not bound by the Cyber Crime Convention and the European Convention on Human Rights, both treaties are important because all Member States of the European Union are contracting parties.

This report does not deal with the different national legislations, although a large part of the legislation on privacy, identity and security is regulated at the national level. The reason is that both EU and international law have already created a certain degree of harmonisation between the Member States on the issues of privacy and identity (first and second pillar, EC law) and security (third pillar, EU law). This implies that the most important principles can be found in the European and international texts.

4.2 Privacy and data protection law

4.2.1 Privacy and data protection

1. *Introduction.* In a democratic constitutional state, there exist two complementary sorts of legal tools which both aim at the same end, namely the control and limitation of power (De Hert/Gutwirth 2003). A distinction must be made between, on the one hand, tools that tend to guarantee the non-interference in individual matters or the *opacity* of the individual and, on the other, tools that tend to guarantee the transparency/accountability of the powerful.[124] Privacy is an example of the first tool and data protection of the second tool.

2. *Limiting or stopping power through opacity tools* Opacity tools protect individuals and their liberty/autonomy against state interference and of interference by other powerful actors. They are linked to the recognition of human rights and a sphere of individual autonomy and self-determination. They set *limits* to the interference of the power with the individual's autonomy. They block or stop the power. They enforce the anonymity of behaviour (e.g., on the Web through approving regulations of techniques of anonymity, pseudonymity, identity management ...).[125] Essential for opacity tools is their *normative nature*: through these tools, the (constitutional) legislator takes the place of the individual as the prime arbiter of acts that infringe on liberty. Through such tools, the legislator enacts hard or clear norms. Choices about the way liberty interests and other interests should be balanced are made in an abstract way.

***3. Channelling power through transparency tools*.** The second set of tools foresees means of control of powers by the people, by controlling bodies and by the other state powers. These tools intend to compel government and private actors to "good practices" by focusing on the transparency of governmental or private decision-making, which is indeed the primary condition for an accountable and responsible form of governance. The system of checks and balances, for example, installs the mutual transparency of state powers. The controllability and accountability of government by the citizens implies free and easy access to government information, the enactment of swift control and participation procedures, the creation of specialised and independent bodies to control and check the doings of government, and so on.

[124] The use of the word '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'.

[125] A good example is the protection of the 'sanctity' or inviolability of the home, which indeed properly expresses the concern for the respect of the individual's autonomy: the public authorities (but also the other citizens) must respect the bounds of the home. A home is inviolable, and any breach of that principle generally engenders criminal prosecution. Once inside a home, people are more free from interference from the government (and others) than outside. A home is a privileged setting. Within a home, each and everyone has the freedom to do as he/she pleases, uninhibited by society's social and moral mores. This doesn't mean that everything happening inside the home is automatically protected. Search warrants can be ordered in criminal cases, but only, in principle, if a series of stringent conditions are met. Crimes and unlawful acts are not condoned because they happen to take place within a home. But because a home is granted a special measure of protection, trespassing by third parties and especially the police and judicial authorities is strictly regulated.

4. *Distinguishing both in the field of privacy and data protection. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.* The tools of opacity are of a different nature than the tools of transparency. Opacity tools embody normative choices about the limits of power, while transparency tools come into play after these normative choices have been made, in order *still* to channel the normatively accepted exercise of power. While transparency tools are thus directed towards the control and channelling of legitimate uses of power; opacity tools protect the citizens against illegitimate and excessive use of power. Opacity tools determine what is in principle out of bounds of government and private actors and, hence, what is deemed so essentially individual that it must be shielded against public and private interference. Transparency tools take into account the fact that the temptations of abuse of power are huge and empower the citizens and special watchdogs to have an eye even on the legitimate use of power: they put counter powers into place. On the one hand, there is a regulated acceptance; on the other, there is a prohibition rule, which is generally subject to exceptions.

These differences appear very clearly if we look at the articles 7 (privacy) and 8 (data protection) of the Charter of Fundamental Rights of the European Union (incorporated in the draft Constitution of the European Union[126]):

> Article 7: "Everyone has the right to respect for his or her private and family life, home and communications".
>
> Article 8: "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority".

These two articles very well express the difference between the two sorts of tools.

Art. 7 provides a good example of an opacity tool because it limits the possible interference with the individual's private and family life, home and communications. In a more general way, it protects the individual’s privacy (or autonomy). It is normative and prohibitive (although of course these prohibitions are not absolute): the rule is a 'no', but exceptions under a number of conditions are thinkable.

[126] The Charter is part of the future constitution. If this constitution enters into force, people will be able to use it to react against Community Institutions before the European Court of Justice. They will also be able to use the rights foreseen in the Charter before a national court, since the constitution will have direct effect.

Art. 8 provides a good example of a transparency tool because it organises the channelling, control and restraint of a power practice, namely the processing of personal data. Data protection legislation regulates, and does not prohibit the processing of personal data. It guarantees control, openness, accountability and transparency of the processing of personal data. In general, data protection does not have a prohibitive nature. The rule is a 'yes', but under conditions. Under the current state of affairs, data controllers (actors that process data) are recognised to have a right to process data relating to others. Hence, data protection is pragmatic in nature: it assumes that private and public actors need to be able to use personal information and that this must be accepted for societal reasons.

5. Privacy as an opacity tool, data protection as a transparency tool. We can thus distinguish privacy protection as an opacity tool and data protection as a transparency tool.

Privacy protects the individual autonomy against steering and ensures the non-interference in individual matters. It protects the individual’s right to be different and his or her autonomy to engage in relationships, their freedom of choice, their autonomy as regards, for example, their sexuality, health, personality building, social appearance and behaviour, and so on. It draws principled normative and often prohibitive limits to interference with these values; but precisely because privacy is also relational and contextual, it is not an absolute value. It can be derived from, as a result of the prevalence of other interests (for example, rights of others, law enforcement, public health, and so on). This can be done on a case by case basis (case law applying art. 8 ECHR, see further sub 9.1.2) or, mainly, by legislation, e.g., in law enforcement and criminal procedure (which then are transparency tools, regulating a regrettable but necessary interference with privacy).

As already said, *data protection* legislation can mainly be seen as a transparency tool because, in principle, it allows the processing of personal data under the conditions of specific procedural safeguards to promote meaningful accountability and to provide individuals with an opportunity to contest inaccurate or unlawful record holding practices (see further sub 7.1.3). Transparency tools are the default tools in all areas of personal data processing.

It must be said, however, that data protection is not only a transparency tool, it also sometimes provides for opacity rules, setting normative limits and prohibitions. To give just one example: a prohibitive rule, a prohibition to process data, applies to “sensitive data” (data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sexual preference). The underlying motive is that the processing of these sensitive data bears a supplementary risk of discrimination. The prohibition is nonetheless never absolute but derogations are (in principle) only possible in strictly defined circumstances, for example, for reasons of national security.[127]

6. Complementary legal tools. Hence, opacity and transparency tools are *complementary legal tools*. Both tools pre-suppose each other. It is thus up to the legislator to consider both tools and to identify the kind of tools necessary for a given problem, especially with regards to technological developments. How much of what tool is necessary and when?

Furthermore, it should be stressed that the two approaches do not exclude each other. They of course depend on policy choices, which can be revised and adapted. As a result, an option for the transparency approach (regulating instead of prohibiting) can after some time and practice eventually show that the opacity approach is preferable (and vice versa) or that a better balance between approaches should be devised. In reality, one will rarely find legal solutions based exclusively upon one tool. A blend of the two approaches will generally be preferable since a solid legal framework should be

[127] Another example can be found in Article 15 of the Data Protection Directive, inasmuch that this article can be construed as the prohibition of decision making affecting persons solely on the basis of profiles. But again, both prohibitive features are accompanied by numerous exceptions that do not set strong limits to the targeted actions.

A third opacity tool in data protection can be found by an interpretation of the purpose specification principle. This principle, at the heart of data protection as it existed in many countries before the European Data Protection Directive came into force, states that the purposes for which personal data are collected should be legitimate and should be specified not later than at the time of data collection. Subsequent use should be limited to the fulfilment of those purposes. Preventive control of the intention of the controller and prohibition of illegitimate use was at the heart of data protection. The idea was not wholly new, since Article 8 ECHR holds that infringements of privacy can only by organised by law for legitimate purposes. In the past, when data were used mostly for only a single purpose, the logic behind the principle could be upheld with not too much difficulty. Today, in the new economy and in a public sector ready for e-government, data are used for multiple purposes and much more intensely and effectively than ever before. Clearly these evolutions have influenced the drafting of the Data Protection Directive.

The fundamental purpose limitation principle is now stated in Article 6 (1b) of the Data Protection Directive. Compared to the situation in, e.g., Belgium, before the Data Protection Directive, the wordings were weaker. It is now said that subsequent use of data should be limited to the fulfilment of the initial purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. This loosening of the purpose specification principle, coupled to the numerous possibilities in the directive to render processing legitimate by obtaining consent, can be interpreted as a shift from prohibitive to channelling logic. Transparency seems to have replaced legitimacy as the core value of data protection. Legitimate might now be interpreted to mean whatever processing that has been rendered transparent.

both flexible (transparency) and firmly anchored in intelligible normative choices (opacity).

A good example of such balancing of approaches is given in the Directive 2002/58/EC on privacy and electronic communications of 12 July 2002 (cf. infra). This directive puts an end to the long lasting controversy regarding direct marketing by explicitly adopting an opt-in system which inherently implies the prohibition of unsolicited marketing mail unless the user explicitly requests to receive it. In this example, it becomes clear how the model of channelling business practices (transparency) is supplemented by the limiting model of a negative obligation (opacity) after due consideration and debate. Another example is provided by the numerous national bills on the use of DNA samples in criminal matters. Although the processing of DNA samples, from the perspective of data protection (Directive 95/46/EC), is in fact an ordinary application of processing of personal data, the inherent risk explains why states supplement general data protection bills with specific prohibitive bills on DNA.

4.2.2 Privacy in art. 8 of the European Convention on Human Rights (ECHR)

1. Introduction. Within the Western legal system, privacy is primarily an issue of international and constitutional law. [128] Privacy is mainly protected by explicit provisions, both in international human rights treaties and in the distinct constitutions. The first provision to mention is article 12 of the 1948 Universal Declaration of Human Rights[129]. Like the whole Declaration, the article is not legally binding for national legal systems, even though it remains a topic of hot debate. Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR) also seeks to protect privacy[130]. And finally, one has to refer to article 8 of the European Convention on Human Rights (ECHR) which highlights the respect for private life in the European human rights order. Both the ICCPR and the ECHR are binding treaties. On top of that,

[128] The right to privacy is also consecrated by numerous national constitutions and by other international legal instruments, such as The Universal Declaration of Human Rights (United Nations, 1948) and the International Covenant on Civil and Political Rights (United Nations, 1966).

[129] Article 12 of the Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[130] Article 17 of the International Covenant on Civil and Political Rights: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

article 17 of the ICCPR and article 8 of the ECHR are self-executing and directly affect the national legal systems. They can both be invoked and have to be applied by national judges. In practice, the ICCPR is overshadowed, certainly when it comes to privacy, by the ECHR. The latter is older, has a strong supranational judicial control mechanism and, last but not least, the Strasbourg Court can boast an impressive list of judgments on privacy. All this makes it legitimate to focus attention on the ECHR.

2. Article 8 ECHR. The ECHR is designed to protect individuals' fundamental rights and freedoms and, as already said, it provides for a judicial procedure which allows individuals to bring actions against governments, if they consider that they are the victims of a violation of the Convention. After the exhaustion of national remedies, individual complainants have direct access to an international court, the European Court of Human Rights in Strasbourg.

Article 8 ECHR, the privacy article of the Convention, states:

> “(1.) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2.) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

This provision (partly copied in Article 7 of the European Union Charter of Fundamental Rights, cf. supra) is the source for EU legislation dealing with privacy and the protection of personal data, as well as of national legislation. Article 8 of the ECHR does not formulate privacy as an absolute right. Exceptions are made possible in the second paragraph of the provision, but the drafters of the Convention took care in providing safeguards against possible abuse of the right to formulate exceptions. According to paragraph 2 the restriction of privacy must be foreseen by law – or an equivalent legal source (the formal criterion); secondly, the restriction can only be applied when it is considered necessary in a democratic society (the necessity criterion); thirdly, it can only be used to achieve one of the specific and limited goals set out in article 8 of the ECHR, including public security and the safeguarding of rights and freedoms of others (the legitimacy criterion); fourthly, the Strasbourg Court has added the condition that any action must be useful, indispensable and proportional to achieve the set goal (the proportionality criterion). The last standard implies that the established goal could not be reached through measures that would have had a lesser impact on the guaranteed freedom of the individual concerned (subsidiarity criterion). If those conditions are met, the authorities can take measures which constitute an invasion of privacy. If not, the Strasbourg Court can rule they contravene the ECHR.

Increased concerns about security have put civil liberties in general and the rights to privacy and the protection of personal data in particular under pressure. These concerns have resulted in numerous national and international security initiatives with a far-reaching impact on human rights. It is very troublesome in this regard that the directive does not apply to the processing of personal data in the course of so-called “third pillar” activities. Only the national constitutional courts and the European Court of Human Rights, next to public upheaval, seem to have enough weight to counterbalance some of the extreme aspects of these initiatives.

Privacy, according to article 8 and its interpretation by the Court of Strasbourg, is a legal concept translating the political endeavor to ensure non-interference in individual matters. As such, it works as a shield and protects the opacity/anonymity of the individual. Art. 8 can thus be invoked against invasions of autonomy and self-determination. Although most of the problems related to AmI will be problems of data protection, the use of invasive technologies might often violate privacy.

Concerning the protection of personal data, article 8 of the ECHR has a number of weaknesses: it does not apply to the private sector (except for the application of the positive obligations doctrine); the right to a private life does not necessarily include all personal data, and so there was the question of whether a large proportion of data would be sufficiently safeguarded, and the right of access to data on oneself is not covered by the concept of the right to privacy as expressed in Article 8 ECHR (Maghiros 2003).

This is, of course, where data protection comes in. Contrary to the ECHR-privacy protection, the European data protection directive applies to all processing of personal data in both the private and the public sector: the complex question "is this a privacy issue?" is then replaced by a more neutral and objective question "are personal data processed?” Once this is the case, data protection applies.

4.2.3 Data protection

4.2.3.1 Introduction: Basics of data protection

The basic practices or principles of data protection are spelled out in the international legal data protection texts produced by institutions such as the Organization for Economic Cooperation and Development (OECD 1980), the Council of Europe (Treaty

108), the UN[131] and the European Union (Directive 95/46/EC). Each of these organisations produced what has become a classic basic data protection instrument, respectively the OECD Guidelines, the Treaty 108 and the Data Protection Directive.[132] The EU has also included the right to data protection in the European Charter of Fundamental Rights (see supra) (Charter of fundamental rights, 2000)

National data protection laws in general provide for a series of rights for individuals such as the right to receive certain information whenever data are collected, the right of access to the data and, if necessary, the right to have the data corrected and the right to object to certain types of data processing. Also, these laws generally demand good data management practices on the part of the data controllers and include a series of obligations: the obligation to use personal data for specified, explicit and legitimate purposes, the obligation to guarantee the security of the data against accidental or unauthorised access or manipulation and, in some cases, the obligation to notify a specific independent supervisory body before carrying out certain types of data processing operations. These laws normally provide specific safeguards or special procedures to be applied in case of transfers of data abroad.

In sum, data protection is not prohibitive. On the contrary, in the public sphere, it is almost a natural presumption that public authorities can process personal data as this is necessary for the tasks they have to perform under statute, since, in principle, public authorities in democratic societies act on behalf of the citizens. The main aims of data protection consist of providing various specific procedural safeguards to protect individuals and of promoting accountability by government and private record-holders. Data protection laws were precisely enacted not to prohibit, but to channel power, viz. to promote meaningful public accountability, and provide data subjects with an opportunity to contest inaccurate or abusive record holding practices. The rationale behind data protection in the public sector is the knowledge that authorities can easily infringe privacy and that in all administrative systems there is an urge to collect, store and use data, an urge which must be curtailed by legal regulation. A similar rationale explains the European option to regulate processing done in the private sector.

[131] The *United Nations Guidelines* are a more recent international instrument: Guidelines concerning computerized personal data files, adopted by the General Assembly on 14 December 1990. We will not further discuss these UN Guidelines, because in Europe they are overshadowed by the other regulations.

[132] This directive has been supplemented by data protection provisions in a number of more specific directives (cf. infra).

Data protection regulations mainly belong to the tools of transparency, as opposed to the protection of privacy that pertain to the tools of opacity. The sheer wordings of the data protection principles (the fairness principle, the openness principle, the accountability principle, the individual participation principle ...) already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice. The data protection regulations created a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal.[133] As such, these regulations implicitly accept that processing of personal data is closely linked to the exercise of power and that it facilitates its establishment.

In what follows, we focus upon the European legislation concerning data protection.

4.2.3.2 Data Protection Directive 95/46

General - application field

This directive, stating in its second consideration that “data-processing systems are designed to serve man”, amplifies the principles of data protection contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Directive 95/46/EC).

The directive reconciles the free flow of personal data between the Member States, with the protection of fundamental rights and freedoms of individuals, notably the right to privacy with regard to the processing of such data.

The challenges for data protection law in relation to AmI concern mainly the reconciliation of the principles of data protection law with the concept of AmI. This challenge emerges because important elements of AmI as well as its supporting technologies show that the AmI system *needs* personal data – and probably profiles to work with. In order to *provide* people *with* information (enhanced goods and services), AmI needs to *have* personal information.[134] It should also be mentioned that the decrease in the cost of these technologies as well as the increasing emergence of customers that are willing to pay for these services are continuing.

[133] An outright processing ban effectively applies only to special categories of sensitive personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

[134] However, this means that not concepts, scenarios, practices and techniques of AmI alone should be tested on their compliance with data protection law; data protection law itself can and should be put into question if necessary, e.g., where some data protection rights can not be reconciled on a reasonable ground with good practices and techniques of AmI that are preferable and desired by the user.

These data protection principles are twofold: On the one hand, there exist obligations on those who are responsible for the processing of personal data and on the other hand, certain rights are conferred to the individuals whose data are collected or processed.

Obligations of the data controller

1. Compliance with conditions for data collection and processing

Any processing of personal data must be lawful and fair to the individuals concerned (article 6.1.a). This is the *fairness principle.*

The processing of personal information occurs often automatically and is non-perceivable for the data subject. The use of cookies[135] shows this clearly. Personal data are often processed by third parties without the data subject even being aware of it. Not only the volume of personal data traffic but also the automatic and the invisible[136] way this happens, increases enormously.

Most networked individuals are prepared to forgo their privacy in return for easier access to goods or services, something which may then make them vulnerable to identity theft.

The rate of personal information abuse grows faster than ever. Identity theft is only one example of possible abuse. Unsolicited electronic information (“spam”) and illegal access to information (“hacking”) are other examples.

Many of the proposals for AmI systems and practices seek to merge databases of personal data held in different governmental and private sector sources. There are not only apparent tensions in developing protocols to join up databases, but also evolutions towards legislation that impose proactive, preventive data retention obligations on Internet service providers. This is about to become reality with the actual Draft legislations on the retention of data.[137]

[135] Small programs which are installed on your computer which register your on-line behaviour and which make you or your computer recognisable upon a new visit. They are recognised to be personal data in the sense of the law on data protection.

[136] Cf. the term *ambient.*

[137] Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.

The personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (although a further processing of the data for historical, statistical or scientific purposes is not considered as incompatible provided that appropriate safeguards are provided by the Member States whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual). This is the *principle of finality* (article 6.1.b).

The data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. This is the *principle of proportionality* (article 6.1.c).

There should be limits to the quantity of collections of personal data. The collections should be proportional compared with the purpose for which the collection took place. How to define or decide which data are necessary and which are not – and therefore extra-proportional? Can law define which data are necessary and which not, or can this be agreed contractually? It is common practice to ask and process more data than necessary, e.g., by giving a person some minor advances like price reductions, etc… One cannot deny that in almost all cases, data subjects are obliged by contractual provisions to give (unnecessary) data away just because they can't refuse practically (although they can theoretically).The proportionality principle is not translated into more concrete legislation, only case law gives in some concrete cases (which are not generally binding) a description of what is proportional in a particular situation and what not.

To be legitimate, personal data may only be processed if the data subject has unambiguously given his consent OR if the processing is necessary for (1) the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or (2) compliance with a legal obligation to which the controller is subject, or (3) protecting the vital interests of the data subject, or (4) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, or (5) the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject (article 7).

Consent by the data subject is defined as 'any freely given, specific, and informed indication of his wishes'. The question is how a free, specific and informed consent can be given in an AmI world. By the intelligent agents? How to organise this "consent" when there is in fact an overall, automatic and continuous registration of data? And, in order to give informed consent, how to organise this information in an understandable and opposable way? Are click-through-contracts like software licence agreements during installation procedures, which nobody reads because they just want to install the product, morally and legally acceptable when it comes to personal data? Has the data subject then been informed and has he given his free consent?

AmI is oriented on human support (e.g., by taking over human actions, by decreasing the human intervention in authentication and identification procedures, by minimising the steps that are necessary to contract), so the obligations to specify and inform people about the purposes of processing and the storage period, the consent principle, can put a difficult burden on the providers of AmI services.

Not only can the procedure of consent create difficulties. Also, relationships between data subjects and data controllers very often are so uneven that the data subject has no other choice than to give his/her consent. Moreover, the individual consent might legitimise practices that can turn out to be collective threats or threats to the public interest. Also here, data protection law may stay too abstract, and control over these practices is difficult.

2. Confidentiality and security

Appropriate technical and organisational measures must be taken, both at the time of the design of the processing system and at the time of the processing itself to ensure an appropriate level of confidentiality and security, taking into account the state of the art and the costs of their implementation in relation to the risks represented by the processing and the nature of the data to be protected (article 16 & 17).

3. Notification to the supervisory authority: openness of the processings (article 18-21)

The notification to the supervisory authority is designed to ensure a disclosure of the purposes and the main features of any processing operation in order to verify that the operation is in accordance with the national measures taken under this directive. The information to be given in the notification shall include at least (1) the name and address of the controller and of his representative, if any; (2) the purpose(s) of the processing; (3) the categories of data subjects and the categories of data processed; (4) the categories of recipients to whom the data might be disclosed; (5) proposed transfers of data to third countries; and (6) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing. Except for (6), this information must be publicized in a public register that may be inspected by any person.

However, exemptions from the obligation to notify or a simplification of the notification may be provided for by Member States.

Sensitive data

According to article 8, processing of so-called sensitive data (‘personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life’) is principally prohibited, unless the data subject has given explicit consent (the word ‘explicit’ being a more strict condition than the word ‘unambiguous’, e.g., in Belgium ‘explicit’ means ‘written’) OR when processing (1) is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards, or (2) is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent, or (3) is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects, or (4) relates to data which are manifestly made public by the data subject or, (5) is necessary for the establishment, exercise or defence of legal claims, or (6) is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

How to deal with the difference between sensitive data (very strongly protected) and other data (less protected)? Does this difference still hold when ambient intelligence combines non-sensitive data and sensitive data?

Rights conferred to individuals

1. The right to be informed (article 10 -11)

Information always to be provided:

In case of collection of data from the data subject, the controller must provide the data subject always with (1) the identity of the controller or his representative and (2) the purposes of the processing for which the data are intended.

Information to be provided if necessary to guarantee a fair processing:

Further information such as (1) the recipients or categories of recipients of the data, (2) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply and (3) the existence of the right of access to and the right to rectify the data concerning him must only be given "in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject".

When the data have not been obtained from the data subject himself but from a third party, the controller or his representative must at the time of undertaking the recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed also provide the data subject with information as described above, including the indication of the categories of data concerned.

2. The right to consult the data (right to access & rectification - article 12)

The data subject has the right to obtain from the controller (1) confirmation as to whether or not data relating to him are being processed, (2) information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed, (3) communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, (4) knowledge of the logic involved in any automatic processing of data concerning him.

The data subject has the right to obtain from the controller (1) the rectification, erasure or blocking of data that are not processed in compliance with the provisions of the directive, in particular because of the incomplete or inaccurate nature of the data. In this case, the data subject has the right to obtain from the controller (2) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out, unless this proves impossible or involves a disproportionate effort.

This individual participation principle is of major importance to keep control in the hands of the data subjects. How to organise this with privacy enhancing technology? Can you oblige technology to implement the rights to access, in other words, can you forbid technology which does not allow the execution of a right to access and rectification in a decent way? How is this access organised?

The principle of the accuracy of the data is not only a legal principle to safeguard privacy and identity, but also a technological necessity: To work effectively, systems need to have a very high percentage of accuracy. Even the slightest error in the system could be catastrophic for large numbers of people. This principle of accuracy is very difficult to achieve in practice: How will bad data be made good? Reparation mechanisms are required which include the restoration of personal and professional reputations, as well as restoring financial losses and credit ratings.

3. The right to object to the processing in certain circumstances (article 14)

The data subject has the right to object at any time to the processing of data relating to him at least in the following three situations: (1) when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, (2) when processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed. However, save when otherwise provided by national law, the data subject can only object to processing of data concerning him in these first two situations when he gives proof of a justified objection, an objection “on compelling legitimate grounds relating to his particular situation”, and (3) when the controller anticipates personal data being processed for the purposes of direct marketing.

Automated individual decisions (article 15)

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. However, a person may nevertheless be subjected to an automated individual decision if that decision is taken (1) 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 (2) is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

Applicable law

Any processing of personal data in the EC must be carried out in accordance with the law of one of the Member States. The applicable criterion is the 'establishment' of the data controller, i.e., "the effective and real exercise of activity through stable arrangements, regardless of the legal form of such an establishment".

There are several situations possible: (1) when the controller is established on the territory of one Member State, the law of that state applies; (2) when he is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable; (3) when the processing of data is carried out by a person established in a third country outside the EC, the processing should be governed by the law of the Member State in which the means used (the equipment) are situated, unless such equipment is used only for purposes of transit through the territory of the EC.

Data controllers should be accountable for complying with measures that give effect to the data protection principles. How should this be organised? The question which national law is applicable in which situation is an important issue and is related not only to data protection, but also to private international law. One is confronted with difficulties when data protection law is not harmonised in places where people move and ambient intelligence is applicable. Which data protection 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? Should data protection not be a personal right instead of a territorial right?

These questions also relate to the approach of data protection on a wider scale: How to bring in line the development of AmI technologies with the principles of a democratic constitutional state in which the public (not really represented by lobby groups) is to be consulted and involved in decision taking?

Third countries

The transfer of personal data to a third country, which does not ensure an adequate level of protection, is prohibited, unless the data subject has given his consent unambiguously to the proposed transfer or unless the transfer is necessary under certain conditions.

The Commission can enter into negotiations with a view to concluding an agreement which ensures that a third country offers an adequate level of protection by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals. An important example of such an agreement is the so-called Safe Harbour agreement, which has been concluded between the USA and the EU. Unlike the EU, the USA uses a sectoral approach that relies on a mix of legislation, regulation and self-regulation. The Safe Harbour agreement aims to ensure the protection of personal data transferred from a European Member State to the USA. The agreement sets out the following principles: notice, choice, onward transfer, security, data integrity, access and enforcement. These principles are completely voluntary, but organisations which wish to obtain and maintain recognition of the fact that they ensure an adequate level of protection for the transfer of data from the EU to the United States must subscribe to these principles, reveal their confidentiality rules and fall within the competence of the Federal Trade Commission or of any other body fulfilling a similar mission (Poullet 2000). The European Commission decided in decision 2000/520/EC (Commission Decision of 26 July 2000) that the "Safe Harbour Privacy Principles" (implemented in accordance with the guidance provided by the frequently asked questions issued by the US Department of Commerce on 21 July 2000) are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States. The Commission also decided that Argentina (Commission Decision C(2003) 1731), Canada (Commission Decision 2002/2/EC)[138] and Switzerland (2000/518/EC) provide an adequate level of protection for personal data transferred from the Community to those countries. The commission is currently looking into the privacy protection schemes in New Zealand, Australia and, Hong-Kong[139].The issue of enforcement is a major problem in international relations and this will increase in an AmI world without physical borders. The system discussed above might be a solution to this problem. It should however be noticed that it does not give a perfect and world wide protection. The Commission has only decided for a limited amount of third countries that they offer an adequate level of protection of the private lives and basic freedoms and rights of individuals. At the other hand, there has been quite some criticism on the safe harbor agreement between the U.S.A. and the E.U. The main criticism is the fact that it relies on a self-regulatory systems whereby companies merely promise not to violate their declared privacy practices[140].

[138] The Commission, however, only recognized the adequate protection only for certain personal data transferred from the European Union to Canada.

[139] http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82589&als[theme]=Privacy %20and%20Human%20Rights%202004#_Toc87939573

[140] http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82589&als[theme]=Privacy%20and %20Human%20Rights%202004#_Toc87939573

The transfer of personal data to a third country which does not ensure an adequate level of protection can be authorised, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses. The Commission decision 2001/497/EC enumerates in its Annex two sets of standard contractual clauses, which are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.

Exclusions from the application field of the directive

Finally, however, the following processing of data is explicitly excluded from the protection offered by this directive: The processing of data… (1) which concerns legal persons; (2) that is carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses; (3) that is carried out for the purposes of public security, defence, national security or in the course of State activities in areas of criminal law and other activities which do not come within the scope of Community law; (4) that are rendered anonymous in such a way that the data subject is no longer identifiable.

So, data protection law does not apply to all kinds of data. Firstly, it only applies to information relating to an identified or identifiable natural person ('data subject'): anonymous data do not fall under the scope of the directive: this means that the principles and safeguards do not apply to anonymous data. Profiles are often built with anonymous data and actions, while actions and decisions by an AmI system can be taken on the basis of such anonymous profile. It is not clear whether and how the data protection directive gives the right to people to object to making their personal data anonymous, while they are processed later as anonymous data and while people are confronted with those anonymous data on the other hand (e.g., when a person falls under a profile, made with anonymous data).[141]

[141] However, the problem of anonymous data can be relative in some circumstances: The notion of 'identifiable' in the European directive is, unlike other international data protection texts, very extensive. Data that at first glance does not 'look' like personal data can very often lead to an individual. It is not because a processor wants data to be anonymous, that data are anonymous. The definition of 'identifiable' is so broad that data can be considered personal as long as the controller himself is still able to identify the persons behind the data. To stay out of reach of European data protection is only possible through achieving maximum anonymity.

Also, the directive protects only natural persons (while the privacy and electronic communications directive protects also legal persons). Questions should be asked whether this distinction still holds in relation with ambient intelligence.

4.2.3.3 Privacy & Electronic Communications Directive 2002/58

As a response to technological developments, Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector translated the principles set out in the data protection directive into specific rules for the telecommunications sector (applying to public telecommunications networks and publicly available telecommunications services such as telephone, mobile networks and Internet related services).

This Directive 97/66/EC has been replaced entirely by Directive 2002/58/EC to reflect new developments in the markets and technologies for electronic communications services, such as the Internet (e-mail, VoIP, chat rooms, ...) and digital mobile networks (mobile communications, SMS, ...) so as to provide an equal level of protection of personal data and privacy, regardless of the technologies used (cf. recitals 4, 5 and 6 of the directive).

1. Application field

Directive 2002/58 provides for specific legal, regulatory and technical provisions for the electronic communications sector.

The directive applies only to public communication services, whereas data protection directive 95/46 applies to both public and non-public communication services. It not only protects fundamental rights and freedoms of natural persons but also protects the legitimate interests of legal persons, whereas directive 95/46 only offers protection to natural persons.

In its recitals, the directive mentions explicitly that Member States, concerned providers and users should co-operate in introducing and developing technologies that apply the guarantees provided for by the directive, taking account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

Also like Directive 95/46, this directive shall not apply to activities concerning public security, defence, state security and the activities of the state in areas of criminal law. It stipulates that Member States may, for reasons of national security, defence, public security and the prevention, investigation and prosecution of criminal offences, enact legislation providing for the retention of traffic and location data, pertaining to all forms of electronic communications, by the telecommunications operators.[142]

Today, there is a draft framework decision on the European agenda, in which communication service providers are obliged to organise data retention – of one to three years – of all traffic and location data concerning mail, Internet and telephone communications on the territory of the EU. Also to be taken into account is Council Regulation 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

2. Security and confidentiality

The *security* obligations of service providers exist in (1) taking technical and organisational measures and (2) informing users and subscribers.

“(1) Service providers should take appropriate technical and organisational measures to safeguard the security of their services, if necessary in conjunction with the network provider and having in regard the state of the art and the cost of their implementation”. According to the recitals, they have also the obligation to take, at their own cost, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service.

(2) In case of a particular risk of a breach of the security of the network, the service provider must inform the subscribers of such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved. This information must be free of charge. According to the recitals of the directive, the service provider must also inform the users and subscribers of Internet communication services of measures they can

[142] This retention possibility has been firmly criticised by EPIC and Privacy International, *o.c.*, 44: "Although this data retention provision is supposed to constitute an exception to the general regime of data protection established by the directive, the ability of governments to compel Internet service providers and telecommunications companies to store all data about all of their subscribers can hardly be construed as an exception to be narrowly interpreted. The practical result is that all users of new communications technologies are now considered worthy of scrutiny and surveillance in a generalized and preventive fashion for periods of time that States’ legislatures or governments have the discretion to determine". These privacy invasive retention schemes were devised in the aftermath of 11 September 2001. Critics also come from Internet service providers who are confronted with the storage and security costs, and from other human rights organisations like Statewatch (*www.statewatch.org*) and EDRI (*http://www.edri.org*).

take to protect the security of their communications, for instance, by using specific software or encryption technologies.

This directive obliges Member States to guarantee the *confidentiality* of communication through national regulations prohibiting any unauthorised listening, tapping, storage or other kinds of interception of surveillance of communications and the related traffic data by persons other than users, without the consent of the users (except when legally authorised to do so). The confidentiality of communications applies both to the contents of communications and to the data related to such communications. Measures must be taken:

(1) To prevent intentional and unintentional unauthorised access to communications

(2) To ensure confidentiality in the course of lawful business practice. In this case, communications can be recorded where necessary and legally authorised for the purpose of providing evidence of a commercial transaction but parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

3. Privacy and identity

Recital 30 of the Directive states in a general way: “Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required”.

3.1. Traffic data

The level of protection of traffic data depends on the purpose of the processing: (1) transmission of communication, (2) billing or (3) marketing electronic communication as well as providing of value added services, e.g., tourist information, route guidance, traffic information and weather forecasts.

(1) For the purpose of the *transmission* of a communication, traffic data relating to subscribers and users may be processed and stored by the service or network provider but must be erased or made anonymous when it is no longer needed for the purpose of

the transmission. The obligation to erase or anonymise traffic data does not conflict with procedures such as caching or using log-in information for access control.

(2) Traffic data, *necessary* for the purposes of subscriber *billing* and interconnection payments, may be processed and stored up to the end of the period during which the bill may lawfully be challenged or payment pursued.

(3) Traffic data, *necessary* for the purpose of *marketing* electronic communications services or for the provision of *value added services*, may be processed by the service provider to the extent and for the duration necessary for such marketing or services, if the subscriber or user to whom the data relate, has given his consent after he has been informed about the type of traffic data processed, the purposes and the duration of the processing. Users/subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

In any of these cases, processing of traffic data must be restricted to what is necessary for the purposes of such activities and must be restricted to persons acting under the authority of the network or service provider. In any of these cases, if data are processed for a longer time than for the transmission, the user or subscriber must be informed of the duration of such processing.

3.2. Location data other than traffic data

Location data other than traffic data are data that “indicate the geographical position of the user without being processed for the purpose of the conveyance of an electronic communication or the billing thereof”.

(1) Such data may only be processed (a) when they are made anonymous or (b) with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a *value added service*.

(2) When consent must be obtained, the service provider must – prior to obtaining the consent – inform the users or subscribers of (a) the type of location data other than traffic data which will be processed, (b) the purposes of the processing, (c) the duration of the processing and (d) whether the data will be transmitted to a third party for the purpose of providing the value added service.

(3) When consent has been obtained, the user or the subscriber (a) shall be given the possibility to *withdraw his consent* for the processing of location data other than traffic data at any time and (b) must continue to have the possibility, using a simple means and free of charge, of *temporarily refusing* the processing of such data for each connection to the network or for each transmission of a communication.

3.3. Cookies and related programs

Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment.

Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and any further use that may be made of those devices during subsequent connections.

The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

3.4. Itemised billing & directories of subscribers

Subscribers shall have the right to receive non-itemised bills.

Subscribers shall be informed, free of charge and before they are included in a directory, of the purposes of such directory. Where printed or electronic telecommunication directories exist, individuals are entitled to refuse to be put on the list, in principle, at no cost (they have the right to determine whether or not their personal data can be included in such a directory).

3.5. Calling identification and automatic forwarding

Where presentation of calling line identification is offered, the service provider must offer both the calling and the called user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification. Conversely, subscribers to this service must have the possibility to reject incoming calls from individuals who have blocked their calling-line identification. Some exceptions are provided for in article 10 of the directive.

Any subscriber must have the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

3.6. Unsolicited communications towards natural persons

The directive also puts an end to the long lasting controversy regarding direct marketing, by explicitly adopting an opt-in system which inherently implies the prohibition of unsolicited marketing mail or communications (Andrews 2002, p. 12): The use of e-communication media such as e-mail and SMS for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent for it (*opt-in*), except where the electronic contacts were obtained directly from the customer in the context of a sale of a product or service for similar products and services, provided that the customer has a clear and easy opportunity to object to such use at the moment of collection and on the occasion of each message (*opt-out*).

4.2.4 Anonymity through privacy and data protection

4.2.4.1 WP 29 Recommendation 3/97: Anonymity on the Internet

This early recommendation by the Article 29 Working Party[143] already points out the dilemma between privacy and security: "It is clear therefore that the question of anonymity on the Internet is at the centre of a dilemma (…). On the one hand the possibility of remaining anonymous is essential if the fundamental rights to privacy and freedom of expression are to be maintained in cyberspace. On the other hand the ability to participate and communicate on-line without revealing one's identity runs against the grain of initiatives being developed to support other key areas of public policy, such as the fight against illegal and harmful content, financial fraud or copyright infringements."

The recommendation mentions the possibility to solve the dilemma between privacy and security on the basis of a 'pseudo-identity' attributed to the users by a specialist service provider. In such cases, while anonymity would normally be respected, if criminal activity were suspected, a link with the true identity of the individual user could be reconstructed.

The recommendation makes a difference between anonymous communication on the Internet (e.g., anonymous re-mailers) and anonymous access to the Internet (e.g., pre-paid cards) and points out the different applications where the issue of anonymity plays a role: e-mail, public discussion fora, www browsing and electronic commerce.

[143] Data Protection Directive 95/46 set up a Working Party on the Protection of Individuals with regard to the Processing of Personal Data, called Article 29 Working Party (WP), composed of a representative of (a) the supervisory authority(ies) designated by each Member State, (b) the Commission and (c) the authority(ies) established for the EC institutions and bodies. The WP has an important advisory status. In addition to other tasks, it advises the Commission on any proposed amendment of the directive on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed EC measures affecting such rights and freedoms. It also can give opinions on codes of conduct drawn up at Community level and make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

The conclusions of the recommendation are:

(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.

This recommendation does not propose concrete measures, but only encourages action on four different levels: the regulatory, technological, economical and 'public awareness' level.

4.3 E-Commerce and consumer protection law

4.3.1 Directive 93/13 on unfair terms in consumer contracts

This directive covers 'the abuse of power by the seller or supplier, in particular against one-sided standard contracts and the unfair exclusion of essential rights in contract'. It only applies to contracts between sellers or suppliers and consumers (natural persons) and in particular, only to contractual terms which have not been individually negotiated by the parties, i.e., when the contract 'has been drafted in advance and the consumer has therefore not been able to influence the substance of the term'. In an AmI world, consumers will become increasingly dependent on services and there is a significant risk that the suppliers of AmI services will obtain an even stronger power position and will abuse it. This supplier should not be allowed to set out privacy conditions which are manifestly not in compliance with the generally applicable privacy rules and which are at the disadvantage of the consumer.

The supplier should also not be allowed to unfairly limit his liability for security problems in the service he provides to the consumer.

The directive imposes mandatory rules of consumer protection, *inter alia,* that contracts should be drafted in plain, intelligible language, that the consumer should be given an opportunity to examine all of the terms and that, if the terms are in doubt, the interpretation most favourable to the consumer should prevail. It might be however difficult to implement those mandatory rules in an AmI world where a large amount of transactions will be concluded instantly and continuously.

The directive includes provisions to avert the risk that the consumer may be deprived of protection under the directive when the other contracting party designates the law of a non-Member country as the law applicable to the contract. The directive contains a list with examples of unfair terms. Although consumer protection organisations have a possibility to ask for the annulment of unfair terms before the competent courts, the directive does not, however, entail prior verification of the general conditions in individual economic sectors.

4.3.2 Directive 97/7 on consumer protection in respect of distance contracts

This directive covers consumer protection regarding distance contracts between suppliers and consumers (natural persons), i.e., 'contracts concerning goods or services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded'. In the e-commerce of today, distance contracts become increasingly important. In an AmI world the majority of contracts will be concluded via distance communications.

This protection exists mainly in the determination of information required to provide to the consumer. Because the information disseminated by certain electronic technologies is often ephemeral in nature 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.

The directive also refers explicitly to the right to privacy and data protection, recognising that intrusive means of communication can be used and that specific limits on the use of such means should be stipulated in the directive (cf. what we know as unsolicited marketing). In an AmI world unsollicited marketing will have an increasingly big impact on privacy and data protection, since services and the communications become more personalised. The marketing could also be used to manipulate the buying behaviour of customers and hence sufficient protection is crucial.

In general, the rules are the following:

Prior to and in good time before the conclusion of any distance contract, the consumer must be provided with the following information in a clear and comprehensible manner and taking into account the principles governing the protection of those who are unable to give their consent, such as minors: identity of the supplier and address in case of advance payment; main characteristics of goods and services; price of goods and services, including all taxes; delivery costs; arrangement of payment, delivery or performance; the existence of a right of withdrawal of at least seven working days; cost of the communication if calculated other than at the basic rate; period for which the offer remains valid; minimum duration of the contract in the case of contracts for the supply of goods or services to be performed permanently or recurrently. In order to obtain a certain AmI service an increasing amount of service providers will be involved and it can be doubted if it will be feasible to provide the required information of all of them. Could we not chose for a solution where you can require this from the service provider to whom you directly pay and who is responsible towards the consumer. How can electronic contracts be concluded through intelligent agents? How can conditions such as consent, information prior to the contract, approval of the goods… be fulfilled?

It is interesting to mention that the right of withdrawal may not be exercised (unless otherwise agreed) in respect of contracts for – *inter alia* – (a) the provision of services if the performance has begun, with the consumer's agreement, before the end of the seven working day period and (b) the supply of goods made to the consumer's specifications or clearly personalised or which, by reason of 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.

The consumer must receive written confirmation or confirmation in another ‘durable medium available and accessible to him’ of the information, during the performance of the contract, and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him. This information must also contain the geographical address of the supplier, information on after-sales services and guarantees and the conclusion for cancelling the contract, where it is of unspecified duration or a duration exceeding one year. Again a problem might arise when several suppliers are involved.

However, the mandatory written confirmation (in a durable, available and accessible medium) does not apply to ‘services performed through the use of a means of distance communication, where they are supplied on only one occasion and are invoiced by the operator of the means of distance communication'. Nevertheless, the consumer must always be able to obtain the geographical address of the supplier to which he may address any complaints.

Because 'the consumer is not in control of the means of communication used', the burden of proof of the information obligations *may be* on the supplier.

The directive contains an article that forbids 'inertia selling' – i.e. the practice of supplying goods or services without their being ordered by the consumer beforehand, where such supply involves a demand for payment – and obliges the Member States to take the necessary measures to exempt the consumer from the provision of any consideration in cases of unsolicited supply, the absence of a response not constituting consent. The user should be allowed to choose which services to accept and to refuse and thus unsolicited services need to be prohibited; especially since in an AmI world payments might happen automatically.

An opt-in rule (prior consent of the user) is provided for use of faxes or automated calling systems, while an opt-out possibility (possible objection of the user) must exist for all other means of communication, through which distance contracts can be concluded. The opt-in rule for unsolicited communication is important to ensure the respect of the consumers' privacy. It should, however, not be limited to faxes and automated calling-systems. Opt-out mechanisms for unsolicited communication are less effective.

4.3.3 E-Commerce Directive 2000/31

This directive was adopted to ensure legal certainty, consumer confidence and free movement of 'information society services' between the EU Member States.

1. The application field of the directive

Information society services, covered by the directive, are defined as “any service *normally* provided for remuneration, at a distance, by electronic means and at the *individual request* of a recipient of services”. In so far as they represent an economic activity, they also extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications or those providing tools for search, access and retrieval of data. Information society services also include services consisting of transmission of information via communication networks, providing access to a communication network or hosting information provided by a recipient of the service.

The use of electronic mail or equivalent individual communications, for instance, by natural persons acting outside their business, trade or profession is not an information society service. The contractual relationship between employers and employees is excluded. Also not information society services are activities which, by their very nature, cannot be carried out at a distance and by electronic means, such as medical advice requiring the physical examination of a patient. In AmI world more and more services will be carried out at a distance and the definition of information society services might change dramatically.

The directive, as stated in recital 14, should be in full compliance with the principles relating to personal data protection, in particular as regards unsolicited commercial communication and the liability of intermediaries. The directive cannot prevent anonymous use of open networks such as the Internet.

2. General information to be provided

Service providers shall render easily, directly and permanently accessible to the recipients of the service (i.e., a natural or legal person using an information society service for the purpose of seeking information or for the purpose of making it accessible) and competent authorities, at least the following information: (a) the name of the service provider; (b) the geographic address at which the service provider is established; (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner; (d) if applicable, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register; (e) if applicable, the particulars of the relevant supervisory authority; (f) in case of a regulated profession, any professional body or similar institution with which the service provider is registered, the professional title, the Member State where it has been granted, a reference to the applicable professional rules in the Member State of establishment and the means to access them; and (g) if applicable, the VAT number. In order to obtain a certain AmI service an increasing amount of service providers will be involved and it can be doubted if it will be feasible to provide the required information of all of the service providers.

3. Information to be provided when contracts are concluded by electronic means

Member States shall ensure, except when otherwise agreed by parties *who are not consumers* (i.e., natural persons who are acting for purposes which are outside his or her trade, business or profession), that the following information must be given by the service provider in a clear, comprehensible and unambiguous way, prior to the order being placed by the recipient of the service: (a) the different technical steps to follow to conclude the contract; (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible; (c) the technical means for identifying and correcting input errors prior to the placing of the order; (d) the languages offered for the conclusion of the contract.

Except when otherwise agreed by parties *who are not consumers*, in cases where the recipient of the service places his order through technological means, the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means (while the order and acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them) and has to make available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order. How can electronic contracts be concluded through intelligent agents? How can conditions such as consent, information prior to the contract, approval of the goods… be fulfilled? It feasible to require every time again a confirmation in an AmI world where services will be continuously ordered.

All these rules (mentioned here above under 3), however, do not apply to contracts concluded *exclusively* by exchange of electronic mail or by equivalent individual communications! But in any of these cases, the contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

4. Unsolicited commercial communication

The directive does not forbid unsolicited commercial communication. However, *if* Member States permit unsolicited commercial communication by electronic mail, they have to ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such, as soon as it is received by the recipient, and that service providers undertaking unsolicited commercial communications by electronic mail, consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves. Consumers should be better protected against spam and unsolicited communications through enforcement; the more, since communications become increasingly personalised. The opt-out registers seem to be insufficient and impractical.

5. Liability of intermediary service providers

In the case of *mere conduit* (i.e., the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, including the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission), a service provider is not liable *for the information transmitted*, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.

In the case of *caching* (i.e., the transmission in a communication network of information provided by a recipient of the service), a service provider is not liable *for the automatic, intermediate and temporary storage of that information*, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that the provider: a) does not modify the information; b) complies with conditions on access to the information; c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

In the case of *hosting* (i.e., the storage of information provided by a recipient of the service), 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 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.

In an AmI world a large number of intermediaries will be involved in providing certain services and thus the question of their liability, and its reach, arises. The directive only stipulates in which case they are not liable and it would be useful to have rules on when they are liable and to what extent they are liable. There should be rules on the liability of information service providers when they violate privacy rules.

4.4 Torts and liability

4.4.1 Directive 85/374 on liability for defective products

This directive consists of the following important concepts: The producer shall be liable for damage caused by a defect in his product. A product is defective when 'it does not provide the safety which a person is entitled to expect, *taking all circumstances into account*, including the presentation of the product, the use to which it could reasonably be expected that the product would be put, when the product was put into circulation'. Although the directive does not foresee this, a product could be considered defective, when it insufficiently protects against privacy violations or when it easily allows identity theft.

The directive installs a 'liability without fault' (or strict liability) which could be '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.' In an AmI world it will become increasingly difficult to prove that you suffered damage because of a fault of the producer.

All producers involved in the production process can be held liable, in so far as their finished product, component part or any raw material supplied by them was defective; where two or more persons are liable for the same damage, they shall be liable jointly and severally, without prejudice to the provisions of national law concerning the rights of contribution or recourse. In an AmI world, an increasing number of producers will provide parts of the final product. When a defective product or services causes damage, it will be difficult to determine which producer to hold liable for the damages. That is why it might be important to hold the producers jointly and severally liable.

The directive also provides: Without prejudice to the provisions of national law concerning the right of contribution or recourse, the *liability of the producer shall not be reduced* when the damage is caused both by a defect in product and by the act or omission of a third party. The liability of the producer may not, in relation to the injured person, be limited or excluded by a provision limiting his liability or exempting him from liability

The directive, however, does not apply to services and it is unclear whether it applies to software. The concepts stipulated in this directive could however be used in a broader context.

4.5 Intellectual Property Rights

4.5.1 Directive 91/250 on the legal protection of software

The legal protection regime for software is of importance to the development of AmI, the implementation of standards and the achievement of interoperability. Although software today seems to become subject matter of patent law[144] – which goes much further in the exclusive appropriation of underlying ideas and principles – copyright law is important too because it expressly allows for what is known as *decompilation*[145].

The directive 91/250, already adopted in 1991, puts the obligation on Member States to protect computer programs by copyright and states clearly that only a specific expression and not the underlying ideas and principles of any element of the computer program are protected.

Exceptions to the exclusive rights of the copyright holders are: (a) reproduction, translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, where these acts are necessary for the use of the computer program (…) including for error correction; (b) making a back-up copy; (c) to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program. These exceptions seem to be insufficient to allow the free use of computer programs required in an AmI world. They, also, can only be invoked by the lawful acquirer, which is a vague term and which could lead to important restrictions.

The directive allows, under certain conditions, *decompilation* of software in order 'to achieve the *interoperability* of an independently created computer program with other programs'. Interoperability is very important in an AmI world. One condition is that the information, obtained through decompilation, will not be used for the development, production or marketing of a program substantially similar in its expression, or for any other act which infringes copyright. An important limitation, however, is the fact that it is only allowed for lawful users, such as licensees.

[144] The Commission has made a very controversial proposal of directive on the patentability of computer-implemented inventions.

[145] Decompilation is the process of using a decompiler to reverse a previous compilation back into its component parts. To decompile is to convert executable (ready-to-run) program code (sometimes called object code) into some form of higher-level programming language so that it can be read by a human. Decompilation is a type of reverse engineering that does the opposite of what a compiler does.

The directive finally obliges the 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 unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program. Privacy enhancing technology might be protected against their circumvention under this provision, since they are often software. An important difference between this directive and directive 2001/29 is that this directive requires that the “sole” intended purposes is circumventing the technical device, while directive 2001/29 requires that it would be “primarily” designed for this purpose. The software directive only protects against the putting in to circulation … of devices which have no other function then circumventing and this is an important limitation. Another important difference is the fact that the directive only protects against the putting into circulation, possession … of these devices and not against the act of circumventing as such. It would be advisable to have a uniform solution which includes the protection of Privacy enhancing technologies.

4.5.2 Directive 96/9 on the legal protection of databases

This directive is important for AmI because most scenarios require the linking and integration of several databases[146] (at the same time) for providing AmI services. The directive foresees a double protection for databases: a copyright protection and a *sui generis* database protection.

Databases are protected by copyright if they, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation. Copyright protection does not apply to databases of which the contents are not selected or arranged through the author’s *own intellectual* creation.

Sui generis database protection provides a *sui generis* intellectual property right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents, to “prevent 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”. Repeated and systematic extraction and/or re-utilisation of *insubstantial parts of the contents* of the database shall not be permitted when it

[146] Databases are defined as collections of independent works, data or other materials arranged in a systematic or methodical way and *individually accessible* by electronic or other means.

implies acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database.

Member States *may stipulate* that lawful users of a database may, without the authorisation of its maker, extract or re-utilise a substantial part of its contents (a) in the case of extraction for private purposes of the contents of a non-electronic database, (b) in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved, (c) in the case of extraction and/or re-utilisation for the purposes of public security or an administrative or judicial procedure. A specific exception could be created for AmI, since requiring authorisation for every single use might hamper the functioning of AmI services.

The term of protection can be renewed automatically, for an unlimited period: Any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection.

4.5.3 Copyright Directive 2001/29 of 22 May 2001

This directive is important for AmI, since copyright and related rights play an important role in protecting and stimulating the development and marketing of new products and services (such as information technology services) and the creation and exploitation of their creative content.

The directive harmonises the three patrimonial rights that a copyright holder can enjoy, the reproduction right, the right of communication to the public and the distribution right. It also reassesses the exceptions to the exclusive rights of the rights holder in light of the new electronic environment. It provides for an exhaustive enumeration of exceptions and limitations to the reproduction right and the right of communication to the public (and to the distribution right). The harmonisation is not absolute, since most exceptions and limitations provided are optional. The Member States are not allowed to provide exceptions other than those enumerated.

An important exception for information technology concerns the exclusive right of reproduction: It allows certain acts of temporary reproduction, which are transient or incidental reproductions, forming an integral and essential part of a technological process and carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made. The acts of reproduction concerned should have no separate economic value on their own.

Protection against circumvention

The directive harmonised the legal protection against circumvention of effective technological measures and against provision of devices and products or services, which effectively restrict acts not authorised by the holders of any copyright, rights related to copyright or the *sui generis* right in databases. Notwithstanding this legal protection, Member shall take appropriate measures to ensure "that the right holders make available to the beneficiaries of an exception or limitation provided for in national law the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned". A similar protection could be provided against the circumvention of privacy enhancing technologies. The Member States also have to provide for an adequate legal protection of rights-management information. This rights-management information could not only be used to ensure that the copyrights are respected, but also to obtain information about the identity and the habits of the users. This information could violate privacy or could be useful for criminals to know when somebody is at home or online.

4.6 I.C.T. law

4.6.1 Electronic signatures

4.6.1.1 9.5.1.1. Directive 1999/93 on electronic signatures

This directive creates a legal framework for electronic signatures and for certain certification services. They are important in an AmI world, since they might allow the use of pseudonyms: Only the certification provider needs to know the identity of the signatory. The party which receives the document with an electronic signature can rely on the certification provider and in case of a legal conflict, the certification provider can exceptionally make the identity of the signatory public. They might also enhance the security of electronic transactions in an AmI world.

To make electronic signatures reliable, they should be certified by professional organisations which ensure that they fulfil the necessary requirements. That is why the directive tries to promote the establishment of certification services providers. To enable them to provide services to other Member States without requiring a specific authorisation every time, the directive provides that these certification service providers will be supervised by their country of establishment.

Next to this supervision mechanism, the directive also deals with the liability of certification service-providers. To further enhance the trust in electronic signatures, the directive enumerates in its annex III the requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures. An appropriate private or public body of a Member State has to check the conformity with these requirements and all other Member States shall recognise such a determination of conformity. The Commission may establish and publish generally recognised standards for electronic-signature products. This publication might solve problems of interoperability. The Member States shall presume compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those (published) standards.

Legal effects of electronic signatures

In an AmI world, electronic signatures can play an important role in the conclusion of contracts, henceforth certainty about their legal value/effect is crucial. The legal effects of electronic signatures depend on whether they are advanced electronic signatures[147] or not. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) 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 (b) are admissible as evidence in legal proceedings. Member States shall 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.

It finally sets out rules concerning certification service-providers in third countries and states that the certification service-providers should respect the rules concerning data protection.

[147] Advanced electronic signatures have to fulfil the following criteria: (a) they are uniquely linked to the signatory; (b) capable of identifying the signatory; (c) created using means that the signatory can maintain under his sole control; and (d) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

4.6.2 Standards and interoperability

4.6.2.1 Directive on technical standards and technical regulations in Information Society Services

Standardisation is quintessential for interoperability. In the several AmI scenarios, many different technologies have to work together and they need to be compatible. Technical standards and regulations could, however constitute barriers to the free movement of AmI services. That is why they are only allowed "where they are necessary in order to meet essential requirements and have an objective in the public interest of which they constitute the main guarantee". To ensure that the standards and regulation meet these criteria, the directive foresees a detailed information procedure. The information procedure could prevent the creation of incompatible standards within the European Union. It should improve both the transparency and legal certainty.

A specific temporary standstill period has been established in order to prevent the introduction of national measures from compromising the adoption of binding Community acts by the Council or the Commission in the same field.

The information and cooperation procedure foreseen in this directive can help the Commission in harmonising the standards and can even form the basis for the creation of European standards.

The directive has been amended by the directive 98/48/EC of 20 July 1998 to add Information Society Services[148].

4.6.2.2 WP 29 Opinion 1/98 on Platform for Privacy Preferences (P3P) and Open Profiling Standard (OPS)

According to this opinion, P3P conceives of privacy and data protection "as something to be agreed between the Internet user, whose data are collected, and the website that collects the data", while the OPS is intended "to provide for secure transmission of a standard profile of personal data".

[148] It defines these services as: "Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". For the purposes of this definition: "At a distance means" that the service is provided without the parties being simultaneously present, "by electronic means" means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means, "at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request.

WP 29 comments on the initiative of the World Wide Web Consortium, which seeks to develop a single vocabulary through which a user's preferences and the site's practices are articulated, based on the philosophy that “the user consents to the collection of his personal data by a site, provided that the site's declared privacy practices, satisfy the user's requirements”. This single vocabulary for privacy Preferences might be very important for AmI, since in order to ensure the respect for privacy and data protection, all participants in the AmI world (suppliers and users) should have a common understanding of the content of privacy and data protection. The opinion, however, states that the vocabulary of P3P has not been developed with reference to the highest known standards of privacy and data protection, but with reference to lower common standards.

Interesting comments are *inter alia*: (a) technical platforms for privacy protection must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and **non-negotiable** level of privacy protection for all individuals and (b) browsing software that is sold or distributed within the EU must be designed and configured so as to ensure that on-line agreements which are in contradiction with prevailing data protection laws are not possible.

Very interestingly, WP 29 refers to the ‘default privacy settings’ for browsers and even implicitly to AmI: “Given that most Internet users are unlikely to alter any pre-configured settings on their browser, the 'default' position regarding a user's privacy preferences will have a major impact on the overall level of on-line privacy protection. P3P and OPS must be implemented into browser technology with default positions which reflect the user's interest to enjoy a high level of privacy protection (including the ability to browse websites anonymously) without finding himself blocked or inconvenienced in his attempts to gain access to sites. Where an operator requests, as a condition for access to his site, the provision of a profile of identifiable data, the user should be asked each time for his consent for the provision of this information to the particular site in question. Where a site does not require such information, access could be seamless.”

The WP encourages the development of Internet software consistent with data protection rules and considers that it would be appropriate to develop mechanisms to verify the conformity of Internet software in this regard.

4.6.3 ICT implants

4.6.3.1 Directive 90/385 on active implantable medical devices

This directive aims at harmonising the level of safety by mandatory specifications relating both to the technical safety features and the inspection procedures for a number of medical devices, including active implantable medical devices and custom-made active implantable medical devices. The directive sets out strict rules applying to active implantable medical devices. In AmI world implantable devices might be used for non medical purposes. In this situation we should create even stricter rules to ensure the safety. The Opinion of European Group on Ethics in Science and New Technologies on the ethical aspect of ICT implants in the human body, stresses the issues and risks when using ICT implants and also points out that there might be serious problems concerning privacy, data protection and identity when using ICT implants.

4.7 Criminal law

4.7.1 Directive 98/84 on the protection of services based on conditional access

The directive deals with the legal protection of all those services whose remuneration relies on conditional access, such as television broadcasting, radio broadcasting and especially information society services. Many services in an AmI world will rely on conditional access and it is important to provide sufficient protection of those services.

It obliges the Member States to prohibit (a) the manufacture, import, distribution, sale, rental or possession for commercial purposes; (b) the installation, maintenance or replacement for commercial purposes; and (c) the use of commercial communications to promote devices, which enable or facilitate without authority the circumvention of any technological measures designed to protect the remuneration of a legally provided service. A similar legal protection could be provided for privacy enhancing technology.

4.7.2 Cybercrime Convention of 23 November 2001

In an AmI world a lot of criminal activity will have a cross border dimension. In order to effectively react to it, there should be a consensus about how to define the criminal offences related to computer data and computer systems. The Cyber crime Convention obliges the Parties to create both the necessary substantive and procedural legislation related to offences against the confidentiality, integrity and availability of computer data and systems, computer related offences, offences related to child pornography and offences related to infringements of copyright and related rights. It also defines the attempt and aiding or abetting the commission of any of the above described offences as a criminal offence. It further obliges the Parties to establish – under certain conditions – corporate liability for the above mentioned offences.

The convention contains specific procedural rules about expedited preservation of stored computer data, production order, search and seizure of stored computer data, real-time collection of computer data and jurisdiction. This preservation and collection of data may, however, create threats to privacy and data protection. This preservation happens without the knowledge of the subject, which implies that he can not consent to it or react to abuses. Another related problem is the fact that the convention puts exorbitant obligations on Internet service providers and intermediaries.

General principles are set out concerning international co-operation, extradition, mutual assistance and spontaneous information. In an AmI world countries will have to cooperate to effectively deal with criminal offences.

4.8 Jurisdiction and applicable law

4.8.1 Convention of Rome on the Law Applicable to Contractual Obligations (EC)

One is confronted with difficulties when data protection law is not harmonised in places where people move and ambient intelligence is applicable. Which data protection 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? Similar problems arise in case of cross border security problems or ID-thefts. The convention of Rome contains specific rules on the applicable law in case of cross border legal issues, but only in contractual relationships and only when the situation involves a choice between the laws of the different contracting parties. The majority of privacy infringements, ID thefts and security violations, however, do not occur in contractual relationships.

The basic principle in this convention is that the contract shall be governed by the law chosen by the parties. To the extent that the law applicable to the contract has not been chosen by the parties, the contract shall be governed by the law of the country with which it is most closely connected. There are, however, exceptions to these general rules in case of specific contracts such as consumer contracts and individual employment contracts.

The directive is based on the territorial right. Should data protection not be a personal right instead of a territorial right? 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. Personal data are linked with identity and the state of a person. Those aspects are partially regulated by the national law of a person. First of all, it is practically possible due to technology (your digital identity decides which law is applicable). Also, it creates certainty because one always knows which law is applicable and one is protected by the law of his country. This approach of law could be a solution in an AmI world without physical borders.

4.8.2 Regulation 44/2001 on jurisdiction and enforcement

In an AmI world transactions are not limited to the national borders of the countries and there is a very big chance that conflicts will arise which have a connection with several countries. In this case it is important to now which court will be competent. This regulation (Regulation 44/2001) aims to unify the rules of conflict of jurisdiction in civil and commercial matters between the EU Member States. It covers both contractual and extra-contractual matters.

Parties can agree on which court or courts of a Member States are to have jurisdiction to settle any dispute between them concerning a particular legal relationship. In order for such an agreement to be valid, it needs to be in writing or evidenced in writing …. It is important to note that any communication by electronic means which provides a durable record of the agreement shall be equivalent to "writing".

Jurisdiction is generally based on the defendant's domicile. There are however special rules for matters relating to a contract, matters relating to torts … In matters relating to contracts, a person may be sued in the courts of the place of performance of the obligation in question. When the matter concerns the sale of goods, the place of performance of the obligation in question shall be the place where, under the contract, the goods were delivered of should have been delivered. In case of the provision of services, the place of performance of the obligation shall be the place where, under the contract, the services were provided or should have been provided. In an AmI world it will, however, be very difficult to determine where the goods or services where delivered (/provided) or should have been delivered. In matters relating to tort, delict or quasi-delict, the person can be sued in the courts of the place where the harmful event occurred or may occur[149]. It will also be very difficult to determine where the harmful event occurred.

[149] The European Court of Justice stated in the Bier Case (C 21/76) that the place where the harmful event occurred should be understood as the place where the damage occurred or the place where the event having the damage as its sequel occurred.

4.9 Antidiscrimination Law

4.9.1 Introduction – non-discrimination as basic principle of EU law

Non-discrimination is one of the fundamental principles of EU law. The Treaty on European Union in Article 6 states that the Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms. This Convention, signed in Rome on 4 November 1950, recognises the principle of equal treatment in Article 14, which prohibits the discrimination on any grounds such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status in enjoyment of rights protected by the Convention. All Member States are Contacting Parties to the Convention. Any discrimination on the basis of the same grounds in enjoyment of rights set forth by law is also forbidden under Protocol No 12 to the Convention. According to the protocol, no one shall be discriminated against by any public authority on any grounds such as mentioned above.

Hence, Article 6 of the Treaty contains an indirect reference to equality. Within the framework of Union law, there are more explicit references. The Treaty establishing the European Community aims to promote the equality between men and woman in all fields covered by the Treaty (Articles 2 and 3), and prohibits any discrimination based on nationality (Article 12). The Community may also take appropriate action to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation (Article 13).

To further reinforce the protection of the fundamental rights, the Charter of Fundamental Rights of the European Union was proclaimed in December 2000. Articles 21 and 23 of the Charter prohibit any discrimination based on any grounds such as sex, race, colour, nationality, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. The Charter of Fundamental Rights of the European Union is not legally binding, but it is already referred to in the case law of the Court of Luxembourg.[150]

[150] On the Charter: García, R.A., 'The General Provisions of the Charter of Fundamental Rights of the European Union', Jean Monnet Working Paper 4/02, (36p.) via www.jeanmonnetprogram.org.; Eriksen, E.O., Fossum, J.E. & Menéndez A. J. (eds.), The Chartering of Europe. The European Charter of Fundamental Rights and its Constitutional Implications, Nomos Verlag, 2003; St. Peers & A. Ward (eds.), The European Union Charter of Fundamental Rights, Oxford, Hart Publishing, 2004, 392p.; Heusel, W. (ed.), Grundrechtcharta und Verfassungsentwicklung in der EU, Köln, Bundesanzeiger

The scope of the European law implementing those provisions is indeed very broad. A number of measures has been enacted to reinforce the equality between men and women, combat racism and xenophobia, create equal opportunities for people with disabilities and in old age, especially via access to employment and occupation, social protection, vocational training, promotion and working conditions, as well as granting access to justice in case of a breach of that rule. Community measures also aim to grant equal access to and supply of goods and services, despite the gender or the racial or ethnic origin.[151]

Non-discrimination is a fundamental principle of the EU. Provisions establishing the principle in EU law have a general character in most cases. They prohibit using some of the characteristics (grounds for prohibited discrimination as enumerated in the legal documents) in decision-making. This principle would apply to the decisions taken in AmI environment as well, including decisions based on large amounts of data (characteristics) and automated decisions. Non-discrimination provisions do not prohibit the use of such data for other purposes (collecting the data or profiling), however, nor do they address possible use of such characteristics, but only the decision actually made. Those are remedied to some extent, however, by the data protection legislation. It establishes a prohibitive and more severe regime for the processing of sensitive data not as an expression of the will to protect privacy, but to remedy the danger processing of data may create for discrimination. On the other hand, anti-discrimination law could also have the ability to fill gaps in the legal provisions of more specific instruments (such as data protection law). Prohibition of discrimination applies to all situations based on the forbidden criteria, those not only in

Verlagsges.mbH., 2002, Band 35 in Schriftenreihe der Europäischen Rechtsakademie Trier, 248p.

[151] As an example of such measures, one could cite Council Directive 97/80/EC of 15 December 1997 on the burden of proof in cases of discrimination based on sex, *OJ L 014 , 20/01/1998 P.6 – 8;* Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, *OJ L 373 , 21/12/2004 P. 37 – 43;* Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, *OJ L 180, 19/07/2000 P. 22 – 26;* Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, *OJ L 303 , 02/12/2000 P. 16 – 22;* Council Directive 86/378/EEC of 24 July 1986 on the implementation of the principle of equal treatment for men and women in occupational social security schemes, *OJ L 225 , 12/08/1986 P. 40 – 42;* Council Directive 76/207/EEC of 9 February 1976 on the implementation of the principle of equal treatment for men and women as regards access to employment, vocational training and promotion, and working conditions, *OJ L 039 , 14/02/1976 P. 40 - 42*

case of the identifiable individuals (which is a limitation the data protection law) but also anonymous members of a group (group profiling)[152].

Development of new technologies may provide benefits, but also produce costs. This highlights the issues of affordability and discrimination, which may emerge from not having equal access to new technologies and services. Although not many, instruments exist within the legal framework of the EU that deal with this social aspect of technology.

4.9.2 Directive 2002/22 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)

Directive 2002/22 (Universal Service Directive) aims to provide a minimum set of services relating to electronic communications networks and services to all end-users at affordable prices. Such affordable prices are set within each Member State and may depart from those resulting from market conditions. Member States are obliged to ensure access to those services (at affordable prices) to all end-users, irrespective of the territory (including geographically isolated areas), and for the elderly, disabled and for peoples with special social needs. Affordability (for instance, with regard to telephone services) also relates to information to the consumer, tariffs meeting the needs of low-income customers and people with special social needs, and the possibility of the consumer to control expenditures.

Chapter II of the Directive contains a list of the universal services that Member States have to provide. They include ensuring that at least one undertaking provides access to the public telephone network following a reasonable request, the quality of speech and data communications (including Internet access), and take into account prevailing technologies available to the majority of end users. As an important service, the Directive mentions access to public pay telephones and uninterrupted access to the emergency services, free of charge. This shall also be ensured for the disabled in a way that addresses their needs. Directory information and enquiry services are part of the universal service obligation. Member States may decide to make additional services publicly available on their own territory.

Also important for our subject matter is the idea in the Directive to foresee a review of the services in light of economic, social and technological developments. Any change

[152] Custer, B., The Power of Knowledge, ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology, 2004, p. 164-165

of scope in universal services shall be subject to the test of services available to the substantial majority of the population, and shall take into consideration whether the lack of availability of such services creates the risk of the social exclusion of those who cannot afford them. Changes in the scope of the universal services or in the technology cannot produce disproportionate financial burden on the undertakings providing services. Costs of such changes shall also not fall unfairly on the consumers in the lower income brackets.

The scope of this directive is limited and obviously not adjusted to the AmI environment. It covers only a few services, as enumerated in chapter II of the directive, which already are the minimum of information society services (like access to the public telephone network). Presumably consideration should be given to some vital AmI services and technologies, such as those that may play an important role in future emergency services.

5 Summary and first conclusions

Ambient intelligence in Europe

Where privacy, identity and security issues have been taken into account in European AmI or AmI-related projects, there is generally good recognition that such issues are important to user acceptance of AmI. Although that is somewhat comforting, one can’t help but wonder whether deployment of AmI will (continue to) proceed anyway. User acceptance is undoubtedly important, as we know from the reluctance that many people have to using their credit cards to make online purchases, but the lack of widespread acceptance hasn’t been enough to deter the implementation of online purchasing services anyway.

In an online mode, the user is (sometimes) conscious of the need to make a deliberate decision with regard to appropriate levels of privacy and security. Such will not necessarily (or even likely) be the case in the instance of ambient intelligence. Indeed, an individual may not even be aware that he is in a space embedded with ambient intelligence. While there are important differences between the cyber world accessed via the fingertips and the hands-free AmI world, some of the work done with regard to online privacy, security, identity, etc will also be relevant to AmI researchers, regulatory authorities and policy-makers.

From our review of projects in Europe, there seems to be some level of agreement with regard to what might be termed principles in regard to privacy, identity, individual security, trustworthiness and the digital divide in connection with the development and deployment of AmI technologies. The Privacy Design Guidelines developed in the AMBIENT AGORAS project are useful and should be taken into account by all AmI designers.

Among the initial principles SWAMI can draw from its review of projects in Europe are the following:

- Privacy considerations should be taken into account and designed in from the start rather than after an AmI technology has been developed or deployed.
- Privacy enhancing technologies should be easy to use and to understand.
- Individuals should be able to specify their privacy preferences.
- Personal data should not be collected unnecessarily (data minimisation).

- In designing any new technology, potential vulnerabilities should be investigated, not only in the technology, but also in the possible cascading or secondary effects that may result from a failure.
- The dependencies between AmI technologies also should be investigated and their consequences for privacy, identity, security, etc.
- The introduction of new security measures should similarly be assessed to determine whether they create insecurities in some other part of the security chain.
- If biometrics are used for identification and authentication, privacy should be considered together with best practices.
- Fixing an identity in one context should not lead to function / mission creep.
- Policy, regulation and technology development should work hand-in-hand and concurrently.
- In consideration of new policies or regulations or alternatives to regulation that may be required as a consequence of the introduction or proliferation of a new technology, impacts should be assessed and stakeholders consulted.
- Policies and regulations should satisfy the interests and concerns of all involved stakeholders as far as possible and to the extent they cannot satisfy some stakeholders, an explanation should be given as to why that is not possible.

ITEA makes an important point when it says the overarching issue for the future of software-intensive systems is *design for change* (DFC), i.e., such systems are always on and subject to continuous modifications in technology, services, terminals, usage. The design for change principle should also be applied to privacy practices, identity management and security as well.

As observed by more than one project, security is essential in all parts of the future network architecture and the challenge for the future security framework is to maintain simplicity and efficiency. The level of offered security should adapt the service needs in terms of user authentication, information encryption, privacy, anonymity, identity management and content delivery. Security threats may have implications for the regulatory framework and research effort and results should be taken into account when reviewing the regulatory framework for electronic communication in 2006.

Although many companies and industry associations claim that they are user-driven or user-centric, one wonders how extensively users are surveyed with regard to whether they really want a new service or a new technology or if they understand the privacy, security, identity implications. In Europe, led by the EC, the UK and a few other Member States, impact assessments and stakeholder consultations are required in advance of significant policy, legislative and regulatory decisions. Industry, especially industry associations, could usefully adopt a similar procedure. In saying so, we recognise that industry is driven by the profit motive and usually for competitive reasons, especially involving proprietary technology, cannot afford to delay introductions of new technologies and services to the market. Nevertheless, where companies collaborate (for example, in platforms) in designing new systems and open standards, comparable impact assessments could do much to allay public concerns about privacy, security and identity protection.

Ubiquitous computing in the United States

Judging by our survey of projects, the US effort in ubiquitous computing seems to be no less than that of Europe in ambient intelligence. As in Europe, a small but significant percentage of projects are devoted to privacy, security and identity concerns. Security of infrastructure (especially the cyber infrastructure, to use the term used by the US National Science Foundation) in the wake of 9/11 is getting lots of airtime.

From the projects, reports and studies reviewed for this deliverable, one can conclude that there is a strong belief in the advance of technology towards an Internet of things, with “intelligence” embedded everywhere. Indeed, sensors and other devices are already embedded in many things and this trend will undoubtedly continue. While there are many benefits from such technological development – for economic growth, convenience, security, individual and social safety, etc – there are also growing concerns about threats to privacy, profiling, surveillance, spamming, identity theft (fraud) and so forth.

Safeguards are being developed. Some safeguards are technological. Others are based on alternatives to regulation, including media watchdogs and consumer awareness and more sensitive business practices. Generally, in the US, personal data collection is based on opt-out rather than opt-in unlike in Europe where opt-in is the default mode. In the instance of opt-in, no data collection, storage and sharing with or selling to third parties is supposed to take place unless the consumer gives his consent. In the instance of opt-out, the consumer must communicate his wish that his data are not to be collected, stored and/or shared (i.e., they will be unless he says they shouldn’t be).

Generally, one could say that an important difference between the US and Europe in regard to protection of personal data is that the US relies much more on a voluntary, self-regulatory approach while European data protection is underpinned by legislation.

It should come as no surprise, therefore, that personal data are abused to a much greater extent in the US than in Europe and that identify theft, while a serious problem in Europe, is much more serious in America.[153]

The ubiquitous network society in Japan

From the survey of Japanese activities aimed at developing the ubiquitous network society by the target date of 2010, it is clear that the issues of privacy and security are as much of a concern in Japan as in Europe and the United States. The issues bubble close to the surface of many projects, studies and technology developments.

Surveys suggest that Japanese consumers want adequate protection of their personal information even if a high percentage don't make much effort to protect themselves. To that extent, Japanese consumers are much like their European and American counterparts.

There are differences between Japan and the United States. In Japan, one does not have the creepy feeling that one is under constant surveillance by government and industry, as is the case in the US. There is no Japanese equivalent of Total Information Awareness or Carnivore (or none at least that has come to light in the media). In America, both government and industry are making major efforts to profile virtually everyone (not just Americans but foreigners coming into the US) and to link all sorts of databases and to use all sorts of surveillance technologies in order to do so.

A second difference is the emphasis on the user terminal. In the United States, there is more emphasis on smart dust and invisible but pervasive computing, which is somewhat reflected in the European notion of ambient intelligence too. In Japan, the emphasis is on a user terminal (based on a 4G mobile) that can do everything – receive TV signals, serve as a biometric authenticator and RFID reader, provide Internet access, download music, take pictures, turn on the cooker, close the garage

[153] See, for example, "What Europe can teach us about identity theft" by Liz Pulliam Weston. MSN Money: "Determining the rate of identity theft in Europe is difficult, and the reason is telling: Data security experts say it's not seen as enough of a problem to warrant a comprehensive survey. The exception is the United Kingdom, where fraud experts estimate 100,000 people, or about 0.17% of the population, fell victim last year to account hijacking, new-account fraud or other types of identity theft. Compare that to the U.S., where a Federal Trade Commission survey found 10 million ID-theft victims a year – or 3.39% of the population." http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P116528.asp

Ms Weston's article appeared before the MasterCard announcement of theft of data relating to some 40 million credit cards. See "Security Breach Exposes Data On Millions Of Payment Cards" by Steven Marlin. *InformationWeek*. 17 June 2005.

door and provide phone service too. This difference in emphasis is more a matter of nuance than a real difference since similar technologies are being pursued in the US, Europe and Japan.

There are many more similarities than differences (even allowing for nuances) in all three places. The notions of overlay architecture, interoperability of networks, interworking of heterogenous devices, those are the same. Privacy and protection of personal information are important issues in all three. The notion of a digital divide and what to do about it gets (some) air time in Europe, America and Japan – maybe not as much as it should, but at least it's on the agenda. The Japanese government though has made it a central issue in its u-Japan policy just as Europe has made it an important issue in its i2010 strategy.

Efforts are being made to find technological solutions to privacy protection, but it's evident that technology alone is not sufficient to instil confidence in consumers. Laws and regulations are needed as are efforts in raising social awareness of measures that individuals and companies ought to take. Vigilance is the price of freedom.

Safeguards for privacy, personal data protection, identity and so on *are* important. Teruyasu Murakami says Japan can arrive at the first phase of the ubiquitous network but it won't arrive at the second phase until it overcomes the vulnerabilities ("the dark side") inherent in a ubiquitous network. Actually, more than the vulnerabilities must be overcome. Trust must be earned, and that's not easy given society's perceptions already (as revealed in the survey carried out for the MIC, details of which can be found in the MIC White Paper).

These sorts of concerns are fanned by stories in the press citing instances of when personal data are compromised. Mention has been made of the theft of Yahoo BB customer account details. Given the media attention which this story attracted in Japan, it's an indication of how easy it is to lose trust. In an effort to restore some goodwill, Softbank (which owns Yahoo BB Japan) apologised for the breach and promised a 500-yen (=3.50 euros) gift certificate to those customers whose personal data were taken. Is that how much our personal data are worth?

One Yahoo BB subscriber thought the amount was derisory, so he decided to sell his name, street address, telephone number, e-mail address and Yahoo Japan ID via Yahoo Japan Auction (operated by another Softbank group company). He soon had more than 300 bidders. The highest bid was 1,509,000 yen (more than €11,000).[154] Is

[154] http://seclists.org/lists/politech/2004/Mar/0034.html

that the real value of our personal data? It still doesn’t seem like that much, but on the other hand, as the seller said, the data in his case had already been used and leaked. Any proceeds from his auction, he said, would go toward the cost of suing Softbank.

While safeguards will help, at the same time, there is a concern and a desire to ensure privacy protection does not become burdensome, that it should be easy to understand and easy to set.

Teruyasu Murakami recommended three very big projects, one of which would deal with protection of information and another with security, but so far they have not happened. But such ideas might still be worth pursuing, particularly when taken in light of the fact that various Japanese organisations and associations (platforms) have American and/or European enterprises as members and state that they engage or participate with other international organisations. That being the case, there would seem to be value and a willingness to explore safeguards at the international level, rather than only at the national level. The only real instance of this is the European Cyber Crime Convention, but it has met with limited success so far. Perhaps it would be useful to consider Mr Murakami’s suggestions at the international level.

Conclusions from the scenario analysis

The main conclusion from the scenario analysis is that ambient intelligence technology violates most of currently existing privacy-protecting borders. First, increased connectivity between people and spaces blurs such physical borders of observability as walls and doors. One old example of doing that are experiments in computer-supported collaborative work, namely, installation of video cameras in offices with the goal to increase awareness between colleagues and make communications between them more natural and more frequent. These experiments have shown that people forget easily about always-on video cameras, especially because the intuitive expectation "If I can not see you, then you can not see me" does not apply to computer-mediated communications (Bellotti 1993), and this threatens personal privacy.

Similar to the experience acquired in computer-supported collaborative work applications, one can expect that increased connectivity of different kinds between different spaces, suggested in AmI scenarios, will present threats to personal privacy, especially because it is not clear whether new technologies will provide a means to escape gracefully from being always connected. By "escape gracefully", we mean that currently a person is always free not to answer a mobile phone call, and nobody knows why: the person can always say that he/she simply did not hear the phone call in a noisy environment or while taking a shower. Thus, a calling person does not feel offended by the fact that his/her call was not answered immediately. Unlike this nice functionality of current mobile phones, the suggested AmI applications, for example, of the kind "to know always where my family members are" or to track mobile workers with the goal of increasing work efficiency don't allow a chance to escape from being always observed and always connected and make people’s lives "transparent" to observers. It is not clear how small personal secrets will be dealt with in such situation, e.g., visiting a drug store on a work route, or visiting a friend of whom a person's family members disapprove.

Second, the physiological sensors, always-on, always attached to a person (whether for the goal of health monitoring or for personalising TV and learning programs), make this person absolutely helpless to hide his/her feelings because feelings can be discovered from changes in physiological parameters (Nasoz 2003). This means that facial expressions don't constitute a natural border protecting true personal feelings anymore.

Third, the blurring of boundaries between time and space (every kind of activity -- household, work, learning, health care etc -- becomes possible at any time, any space), recording and storing of many kinds of information in AmI systems and increased capacity of data mining algorithms (which enable the finding of relationships and connections between diverse and seemingly unrelated pieces of data) violate personal expectations about spatial and temporal privacy-protecting borders, as well as expectations concerning ephemerality and transience of events.

Another important conclusion from reading AmI scenarios is that it is assumed that AmI technology is accepted by everybody and is available to everybody, and it is never described in the scenarios what happens to people who are either not willing or not able to use Ami technology. Generally, many scenarios pay little attention to the fact that people can have conflicting interests, and underestimation of diversity of humans' interests and desires can present problems.

Another observation from reading scenarios is that many of them present people (children particularly) as passive consumers accepting happily increased dependability on AmI systems and increased superiority of AmI systems and relying on its reminders, surveillance, entertainment and provided comfort more and more, while AmI itself is problem-free and capable of taking such responsibilities. This vision does not seem realistic because AmI systems can not be absolutely problem-free. It is also questionable how people will accept superiority of technology and how the new technology will impact human nature (e.g., why train one’s memory if AmI gives reminders?). This question is especially important to consider when designing AmI support for children, e.g., how to give them new responsibilities and to help in personal development when AmI takes many of their current household duties and responsibilities, provides an attractive gaming environment instead of real life challenges and eases learning by adjusting course material to personal abilities.

Last, it is absolutely unclear from the scenarios how AmI systems are maintained and how it is guaranteed that nobody can manipulate AmI systems for own benefit, e.g., that information about politics, shops, medicines etc is objective.

New technologies should inevitably change personal expectations concerning privacy generally. Nissenbaum (2004) cites a UScourt decision as an example of such changes. The court decided that the police did not violate personal private space when they discovered an illegal activity while flying an airplane over a person’s home and yard, because one can not expect reasonable privacy from surveillance planes since flights have become a common part of our lives. So, what kind of changes in privacy expectations will replace the current expectations when AmI technology becomes a common part of our lives? Whatever they will be, changes in people's expectations of privacy will happen more slowly than technology capabilities grow, as experiments in computer-supported collaborative work have shown. Thus, one cannot help but wonder whether, in future, people will have secrets and whether it will ever be possible to be "left alone".

5.1 Conclusions from the legal analysis

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 most of the problems related to AmI will be problems of 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 discussed in the overview of legal issues is the Safe Harbour agreement concluded between the U.S.A. and the European Union.

When discussing E-commerce and consumer protection law, the legal overview first studied **Directive 93/13 on unfair terms in consumer contracts**. This is important for AmI, since consumers will become increasingly dependent on services and there is a significant risk that the suppliers of AmI services will obtain – in the future – a stronger power position 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. This obligation might encounter certain problems in an AmI world. The **e-commerce directive 2000/31** sets out rules concerning unsolicited commercial communications and concerning the liability of the intermediary services 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. An exception could be created, when the use of parts of the database is necessary in order to deliver or enjoy 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 might enhance the security of electronic transactions in an AmI world. The obligation in the directive to publish generally recognised standards might solve problems of interoperability. Another important legal document concerning standard 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 Cyber crime 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 (data protection) 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. 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**, which aims at unifying the rules of conflict of jurisdiction in civil and commercial matters, is not sufficiently adapted to an AmI world.

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 which 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.

References

Literature

Aarts, E.; Marzano, S. (Eds.) (2003): The New Everyday: Views on Ambient Intelligence. Rotterdam: Uitgeverij 010 Publishers.

Accenture; CERIAS (2001). CERIAS Security Visionary Roundtable: Call to Action. West Lafayette, IN: Center for Education and Research in Information Assurance and Security, Purdue University.

Ackerman, M. S. (2004): Privacy in pervasive environments: next generation labelling protocols. In: Personal and Ubiquitous Computing 8, No. 6, pp. 430-439.

Åkesson, K.-P.; Humble, J.; Crabtree, A.; Bullock, A. (2001). Usage and Development Scenarios for the Tangible Toolbox. ACCORD Deliverable D1.3. Kista: Swedish Institute of Computer Science.

Alahuhta, P.; Jurvansuu, M.; Pentikäinen, H. (2004). Roadmap for network technologies and service. Tekes Technology Review 162/2004. Helsinki: Tekes.

Albrecht, K. (2002): Supermarket Cards: The Tip of the Retail Surveillance Iceberg. In: Denver University Law Review, no. 79, pp. 534-539, 558-565.

Andrews, S. (Ed.) (2002): Privacy and human rights 2002. Washington D.C., London: Electronic Privacy Information Center (EPIC), Privacy International. *http://www.privacyinternational.org/survey/phr2002/*

Antifakos, S.; Michaehelles, F.; Schiele, B. (2002): Proactive Instructions for Furniture Assembly. In: Borriello, G.; Holmquist, L. E. (Eds.): Proceedings of the 4th International Conference on Ubiquitous Computing (Ubicomp 2002). Berlin und Heidelberg: Springer-Verlag (Lecture Notes in Computer Science, 2498).

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

Bardram, J. E. (2004): The Personal Medical Unit -- A Ubiquitous Computing Infrastructure for Personal Pervasive Healthcare. In: UbiHealth 2004 - The 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Nottingham, 7 September 2004.

Becker, T. J. (2004): Aging in Place with Technology: Study Reveals Older Adults will Sacrifice Some Privacy to Remain in their Homes Longer. In: Georgia Tech Research News, 6 May 2004. http://www.gtresearchnews.gatech.edu/newsrelease/privacy.htm

Beckwith, R. (2003): Designing for Ubiquity: The Perception of Privacy. In: IEEE Pervasive Computing 2, No. 2, pp. 40-46.

Bellotti, V.; Sellen, A. (1993): Design for Privacy in Ubiquitous Computing Environments. In: Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93): Kluwer, pp. 77-92.

Beumer, M.; Veldhuis, R. N. J.; Bazen, A. M. (2004): Transparent face recognition in the home environment. In: ProRISC 15th Annual Workshop on Circuits, Systems and Signal Processing, November 25-26 2004, Veldhoven, The Netherlands.

Björk, S. (2002): Designing Mobile Ad Hoc Collaborative Applications: Scenario experiences with Smart-Its. In: Proceedings of ACM SIGCHI Annual Conference on Human Factors in Computing Systems, April 20 - 25, Minneapolis, Minnesota, USA (CHI 2002). http://www.tii.se/play/publications/2002/smartits.chi.pdf

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., Rohs, M., (2005) Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing, In: W. Weber, J. Rabaey, E. Aarts (Eds.): Ambient Intelligence. Springer-Verlag, pp. 5-29, 2005.

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

Crabtree, A.; Rodden, T.; Hemmings, T.; Benford, S. (2003): Finding a place for UbiComp in the home. In: Proceedings of the 5th International Conference on Ubiquitous Computing, Seattle. Berlin, Heidelberg: Springer, pp. 208-226.

Custers, B. (2004): The Power of Knowledge: Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Nijmegen: Wolf Legal Publishers.

Da Costa, O.; Boden, M.; Punie, Y.; Zappacosta, M. (2003): Science and Technology Roadmapping from Industry to Public Policy. In: The IPTS Report 73, pp. 27-32.

Dash, E.; Zeller Jr., T. (2005): MasterCard Says 40 Million Files Put at Risk. In: The New York Times, 18 June 2005.

De Hert, P.; Gutwirth, S. (2003): 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 Homme Affairs (LIBE). Seville,: Institute for Prospective Technological Studies (IPTS Technical Report, EUR 20823 EN), pp. 111-162. *ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf*.

Eggermont, L. D. J. (2002): Embedded Systems Roadmap 2002: Vision on technology for the future of PROGRESS. Utrecht: STW Technology Foundation/PROGRESS.

Ellis, R., ed. (2004). Work/home boundaries and user perceptions of AmI: key issues and implications for business. Project Report EDIN 0453-1302. Heidelberg: Eurescom.

ePOCH (2003). e-ID and the Information Society in Europe. White Paper. http://www.eepoch.net/documents/public/WhitePapers/eepoch_white_paper.pdf.

Eriksen, E. O.; Fossum, J. E.; J., M. A. (Eds.) (2003): The Chartering of Europe. The European Charter of Fundamental Rights and its Constitutional Implications. Baden-Baden: Nomos.

European Commission (2001). Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298 final. Brussels.

European Commission (2002): eEurope 2005: An information society for all. An Action Plan to be presented in view of the Seville European Council. COM (2002) 263 final. Brussels.

European Commission (2003a). 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.

European Commission (2003b): IST 2003: The Opportunities Ahead. Luxembourg: Office for Official Publications of the European Communities.

European Commission (2003c). Electronic Communications: The Road to the Knowledge Economy. COM (2003) 65 final. Brussels.

European Commission (2004a). Science and technology, the key to Europe's future - Guidelines for future European Union policy to support research. COM(2004) 353 final. Brussels. ftp://ftp.cordis.lu/pub/era/docs/com2004_353_en.pdf

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

European Commission (2005a). i2010 – A European Information Society for growth and employment. COM (2005) 229 final. Brussels.

European Commission (2005b). 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.

Fitton, D.; Cheverst, K.; Finney, J.; Dix, A. (2004): Supporting Interaction with Office Door Displays. In: Workshop on Multi-User and Ubiquitous User Interfaces (MU3I) at IUI/CADUI, Madeira.

Friedewald, M. (2005): Safeguards in a World of Ambient Intelligence: Outline of a research agenda on the European Level. In: Hutter, D.; Ullmann, M. (Eds.): Security in Pervasive Computing. Proceedings of the 2nd International Conference, SPC 2005, Boppard, Germany, April 6-8, 2005. Heidelberg, Berlin: Springer (Lecture Notes in Computer Science, 3450), pp. 63-69.

Friedewald, M.; Da Costa, O. (2003). Science and Technology Roadmapping: Ambient Intelligence in Everyday Life (AmI@Life). Working Paper. Seville: Institute for Prospective Technology Studies IPTS.

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

Garate, A.; Lucas, I.; Herrasti, N.; Lopez, A. (2004): Ambient Intelligence Technologies for Home Automation and Entertainment. In: EUSAI 2004, Workshop "Ambient Intelligence Technologies for Well-Being at Home", Eindhoven University of Technology, The Netherlands.

García, R. A. (2002). The General Provisions of the Charter of Fundamental Rights of the European Union. Jean Monnet Working Paper 4/02. http://www.jeanmonnetprogram.org.

Garlan, D.; Siewiorek, D.; Smailagic, A.; Steenkiste, P. (2002): Project Aura: Toward Distraction-Free Pervasive Computing. In: IEEE Pervasive Computing 21, No. 2, pp. 22-31.

Gellersen, H., ed. (2002). Scenarios: Methods and Results. Smart-Its Project Deliverable 4. Lancaster University. http://www.smart-its.com/

Grimm, R.; Davis, J.; Lemar, E. et al. (2004): System support for pervasive applications. In: ACM Transactions on Computer Systems 22, No. 4, pp. 421-486.

Gustavsson, P.; Lundin, J.; Nulden, U.; Taghizadeh, F. (2001): Mobile Scenarios: Supporting Collaborative Learning among Mobile People. In: Proceedings of IRIS 24, Ulvik, Norway, pp. 59-72.

Harmon, A. (2003): Lost? Hiding? Your Cellphone Is Keeping Tabs. In: New York Times, 21 December 2003..

Harrop, P. (2005): Item level RFID: The business benefits of the "tag everything" scenario. Cambridge: IDTechEx Ltd.

Heinonen, S. (2004): Mobile Telework at the Crossroads of Social, Environmental and Cultural Challenges. In: 9th International Telework Workshop, Creete, Greece, 2004.

Hengartner, U.; Steenkiste, P. (2004): Implementing access control to people location information. In: Proceedings of the ninth ACM symposium on Access control models and technologies, pp. 11-20.

Heusel, W. (Ed.) (2002): Grundrechtcharta und Verfassungsentwicklung in der EU. Köln: Bundesanzeiger Verlag (Schriftenreihe der Europäischen Rechtsakademie Trier, 35).

Huizenga, J., ed. (2003). Roadmap for Advanced Research in Privacy and Identity Management. RAPID Deliverable RD 3.0. Delft: TNO-FEL. https://rami.jrc.it/roadmaps/rapid/overall.pdf.

Humble, J.; Crabtree, A.; Hemmings, T. et al. (2003): "Playing with your bits": user-composition of ubiquitous domestic environments. In: Proceedings of the 5th International Conference on Ubiquitous Computing, Seattle. Berlin, Heidelberg: Springer, pp. 256-263.

IST Advisory Group (2002). Trust, dependability, security and privacy for IST in FP6. Luxembourg: Office for Official Publications of the European Communities. http://www.cordis.lu/ist/istag-reports.html.

IST Advisory Group (2003). Ambient Intelligence: From Vision to Reality. For participation – in society and business. Luxembourg: Office for Official Publications of the European Communities. http://www.cordis.lu/ist/istag-reports.html.

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

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

Ito, M.; Iwaya, A.; Saito, M. et al. (2003): Smart Furniture: Improvising Ubiquitous Hot-spot Environment. In: Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03), 19–22 May 2003, Providence, RI: IEEE Press, pp. 48-53.

Jafari, R.; Dabiri, F.; Sarrafzadeh, M. (2004): Reconfigurable Fabric Vest for Fatal Heart Disease Prevention. In: UbiHealth 2004 - The 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications.

Jansson, C. G.; Jonsson, M.; Kilander, F. et al. (2001). Intrusion scenarios in meeting contexts. FEEL Deliverable D5.1. Kista: Royal Technical University. http://dsv.su.se/FEEL/zurich/Item_3-Intrusion_scenarios_in_meeting_contexts.pdf.

Jernström, H. (2002): SiSSy – Smart-its child Surveillance System. In: Ljungstrand, P.; Holmquist, L. E. (Eds.): Adjunct Proceedings of the Forth International Conference on Ubiquitous Computing (Ubicomp 2002). Göteborg: Viktoria Institute, pp. 37-38.

Juels, A.; Molnar, D.; Wagner, D. (2005). Security and Privacy Issues in E-passports. ePrint Archive Cryptology Report 2005/095. http://eprint.iacr.org/.

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

Kato, U.; Hayashi, T.; Umeda, N. et al., eds. (2004). Flying Carpet: Towards the 4th Generation Mobile Communications Systems. Ver. 2.00. 4th Generation Mobile Communications Commitee.

Kawahara, Y.; Minami, M.; Saruwatari, S. et al. (2004): Challenges and Lessons Learned in Building a Practical Smart Space. In: The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 22-26 August 2004, Boston, Mass., pp. 213- 222.

Kent, S. T.; Millett, L. I. (Hrsg.) (2003): Who Goes There? Authentication Through the Lens of Privacy. Washington, DC: National Academies Press.

Kim, S. W.; Kim, M. C.; Park, S. H. et al. (2004): Gate reminder: a design case of a smart reminder. In: Benyon, D.; Moody, P. et al. (Eds.): Proceedings of the Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, Cambridge, MA, USA, August 1-4, 2004. ACM, pp. 81-90.

Knospe, H.; Pohl, H. (2004): RFID Security. In: Information Security Technical Report 9, No. 4, S. 30-41.

Krikke, J. (2005): T-Engine: Japan’s Ubiquitous Computing Architecture Is Ready for Prime Time. In: Pervasive Computing 4, No. 2, pp. 4-9.

Lahlou, S.; Jegou, F. (2003). European Disappearing Computer Privacy Design Guideslines v1. Ambient Agora Deliverable D15.4. Electricité de France.

Langheinrich, M. (2001): Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In: Abowd, G. D.; Brumitt, B. et al. (Hrsg.): Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001). Berlin und Heidelberg,: Springer-Verlag (Lecture Notes in Computer Science, 2201), pp. 273-291.

Langheinrich, M. (2003): The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects. In: Designing for Privacy Workshop. DC Tales Conference, Santorini, Greece. www.vs.inf.ethz.ch/publ/papers/dctales-privacy.pdf

Lashina, T. (2004): Intelligent Bathroom. In: EUSAI 2004, Workshop "Ambient Intelligence Technologies for Well-Being at Home", Eindhoven University of Technology, The Netherlands.

Luff, P.; Heath, C.; Norrie, M. et al. (2004): Only touching the surface: creating affinities between digital content and paper. In: Proceedings of the 2004 ACM conference on Computer supported cooperative work, Chicago, IL, 8th – 10th November 2004pp. 523-532.

Ma, J.; Yang, L. T.; Apduhan, B. O. et al. (2005): Towards a Smart World and Ubiquitous Intelligence: A Walkthrough from Smart Things to Smart Hyperspaces and UbicKids. In: International Journal of Pervasive Computing and Communications 1, No. 1.

Maghiros, I., ed. (2003). 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 Homme Affairs (LIBE). IPTS Technical Report EUR 20823 EN. Seville: Institute for Prospective Technological Studies. ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf.

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

Masera, M.; Bloomfeld, R. (2003). A Dependability Roadmap for the Information Society in Europe. AMSD Delilverable D1.1. https://rami.jrc.it/roadmaps/amsd.

Matthews, T.; Gellersen, H.; van Laerhoven, K.; Dey, A. (2004): Augmenting Collections Of Everyday Objects: A Case Study of Clothes Hangers as an Information Display. In: Ferscha, A.; Mattern, F. (Eds.): Pervasive Computing, Proceedings of the Second International Conference, PERVASIVE 2004, Vienna, Austria, April 21-23, 2004. Heidelberg, Berlin: Springer (Lecture Notes in Computer Science, 3001), pp. 340-344.

Merritt, R. (2004): Homeland Security agency focuses R&D on sensor nets. In: EE Times, 5 Jan 2004. http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=18310807

MIC, Ministry of Internal Affair and Communications of Japan (2005): "Policy Roundtable for Realizing a Ubiquitous Network Society" Compiles Final Report. In: MIC Communication News 15, No. 19-20, pp. 3-5.

Michahelles, F.; Matter, P.; Schmidt, A.; Schiele, B. (2003): Applying Wearable Sensors to Avalanche Rescue: First Experiences with a Novel Avalanche Beacon. In: Computers & Graphics 27, No. 6, pp. 839-847.

Morganti, F.; Riva, G. (2005): Ambient Intelligence for Rehabilitation. In: Riva, G.; Vatalaro, F. et al. (Eds.): Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction. Amsterdam: IOS Press (Studies in New Technologies and Practices in Communication, 6), pp. 281-292.

MPHPT, Ministry of Public Management Home Affairs Posts and Telecommunications of Japan; Economic Research Office General Policy Division (2004). Information and Communications in Japan: Building a Ubiquitous Network Society that Spreads Throughout the World. White Paper. Tokyo. http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2004/2004-index.html.

MPHPT, Ministry of Public Management Home Affairs Posts and Telecommunications of Japan (2004): "Policy Roundtable for Realizing Ubiquitous Network Society" Held. In: MPHPT Communication News 14, No. 23.

Murakami, T. (2003). Establishing the Ubiquitous Network Environment in Japan: From e-Japan to U-Japan. NRI Paper 66. Tokyo: Nomura Research Institute. http://www.nri.co.jp/english/opinion/papers/2003/pdf/np200366.pdf.

Murakami, T.; Fujinuma, A. (2000). Ubiquitous Networking: Towards a New Paradigm. NRI Paper 2. Tokyo: Nomura Research Institute. http://www.nri.co.jp/english/opinion/papers/2000/pdf/np200002.pdf.

Mynatt, E. D.; Essa, I.; Rogers, W. (2000): Increasing the opportunities for aging in place. In: Proceedings on the 2000 Conference on Universal Usability (CUU'00), Arlington, Virginia: ACM Press, pp. 65 - 71.

Nasoz, F.; Alvarez, K.; Lisetti, C.; Finkelstein, N. (2003): Emotion Recognition from Physiological Signals for User Modelling of Affect. In: Proceedings of the 3rd Workshop on Affective and Attitude User Modelling (Pittsburgh, PA, USA, June 2003).

National Research Council; Committee on Radio Frequency Identification Technologies (2005): Radio Frequency Identification Technologies: A Workshop Summary. Washington, D.C.: National Academies Press.

National Research Council; National Academy of Sciences (2001): Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers. Washington, D.C.: National Academy Press.

Neustaedter, C.; Greenberg, S. (2003): The Design of a Context-Aware Home Media Space: The Video. In: Video Proceedings of Fifth International Conference on Ubiquitous Computing (UbiComp 2003).

Ninomiya, S. (2005): Policy and Regulatory Update by Japan. In: APEC Telecommunications and Information Working Group. 31st Meeting. Bangkok. 3-8 April 2005.

Nissenbaum, H. (2004): Privacy as Contextual Integrity. In: Washington Law Review 79, No. 1, pp. 101-139.

Norman, D. A. (1998): The Invisible Computer: Why Good Products Can Fail, the Personal Computer Is So Complex, and Information Appliances Are the Solution. Cambridge, Mass.: MIT Press.

O'Brien, K. A.; Ligtvoet, A.; Rathmell, A.; MacKenzie, D. (2003). Using scenarios to support critical infrastructure analysis and Assessment. ACIP Deliverable D 3.4. Leiden: RAND Europe. http://www.iabg.de/acip/doc/wp3/D3_4_Scenarios_v3_formatiert.pdf.

OECD (1980): OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 September 1980. In: Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. Paris: Organisation for Economic Co-operation and Development, pp. 9-12.

Oertel, B.; Wölk, M.; Hilty, L. M. et al. (2004): Risiken und Chancen des Einsatzes von RFID-Systemen: Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Ingelheim: SecuMedia.

Orr, R. J.; Raymond, R.; Berman, J.; Seay, F. (1999). A System for Finding Frequently Lost Objects in the Home. Technical Report 99-24. Graphics, Visualization, and Usability Centre, Georgia Tech.

Palmas, G.; Tsapatsoulis, N.; Apolloni, B. et al. (2001). Generic Artefacts Specification and Acceptance Criteria. Oresteia Deliverable D01. Milan: STMicroelectronics s.r.l.

Peers, S.; Ward, A. (Eds.) (2004): The European Union Charter of Fundamental Rights. Oxford: Hart Publishing.

Poullet, Y. (2000): Les Safe Harbor Principles - Une protection adéquate? In:, Conférence de l'IFCLA "Le droit de l'informatique au tournant du millénaire", Paris, June 15 and 16 2000. http://www.juriscom.net/uni/doc/20000617.htm.

President's Information Technology Advisory Committee (PITAC) (2005). Cyber Security: A Crisis of Prioritization - A Report to the President. Arlington, VA: National Coordination Office for Information Technology Research and Development. http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

Price, S.; Rogers, Y. (2004): Let's get physical: the learning benefits of interacting in digitally augmented physical spaces. In: Computers and Education 43, No. 1-2, pp. 137 - 151 .

Punie, Y. (2005): The future of Ambient Intelligence in Europe: The need for more Everyday Life. In: Communications and Strategies 57, pp. 141-165.

Rejman-Greene, M., ed. (2003). Final Report of the Roadmap Task. BIOVISION deliverable D2.6/Issue 1.1. Ipswich: BTExact. http://www.eubiometricsforum.com/dmdocuments/BIOVISION_Roadmap.pdf.

Ricadela, A. (2005): Sensors Everywhere. In: InformationWeek, 24 January 2005. http://www.informationweek.com/story/showArticle.jhtml?articleID=57702816&pgno=2

Riva, G. (2003): Ambient Intelligence in Health Care. In: CyberPsychology and Behavior 6, No. 3, pp. 295-300.

Rodden, T.; Crabtree, A.; Hemmings, T. et al. (2004): Configuring the ubiquitous home. In: Darses, F.; Dieng, R. et al. (Eds.): Cooperative Systems Design: Scenario-Based Design of Collaborative Systems. Amsterdam: IOS Press, pp. 227-241.

Sachinopoulou, A.; Mäkelä, S.; Järvinen, S. et al. (2005): Personal video retrieval and browsing for mobile users. In: 17th International Symposium Electronic Imaging Science and Technology, 16-20 January 2005, San José, CA.

Sastry, S. (2003). Testimony and Statement for the Record by Shankar Sastry, Chairman, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley. Hearing on “Cybersecurity: Getting it Right” Before the Subcommittee on Cybersecurity, Science, Research and Development, Committee on Homeland Security, United States House of Representatives. Washington.

Savidis, A.; Lalis, S.; Karypidis, A. et al. (2001). Report on Key Reference Scenarios. 2WEAR Deliverable D1. Heraklion: Foundation for Research and Technology Hellas, Institute of Computer Science.

Schneider, F. B. (Ed.) (1999): Trust in Cyberspace. Washington, D.C.: National Academy Press.

Schneier, B. (1999): Risks of Relying on Cryptography. In: Communications of the ACM 42, No. 10, pp. 144.

Schneier, B. (2004): Customers, Passwords, and Web Sites. In: IEEE Security & Privacy Magazine 2, No. 5, pp. 88.

Schneier, B. (2004): Secrets and Lies: Digital Security in a Networked World. New York, Chichester: Wiley.

Schoenberger, C. R. (2002): RFID: The Internet of Things. In: Forbes Magazine vom 18 March 2002. http://www.forbes.com/global/2002/0318/092.html

Schwarz, J. (2003). Statement of John Schwarz, President, Symantec Corporation on Worms, Viruses and Securing Our Nation's Computers. House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Washington. http://reform.house.gov/UploadedFiles/Schwarz-v5.pdf (accessed 10 January 2004)

Shoji, T.; Nakajima, T. (2004): Privacy-Concern for Context-Aware Environments. In: Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems, May 11 - 12, 2004, Vienna, Austria. http://www.dcl.info.waseda.ac.jp/publications/ic2004-privacy-concern.html.en

Singer, I. (2001): Privacy and Human Nature. In: Ends and Means 5, No. 1. http://www.abdn.ac.uk/philosophy/endsandmeans/vol5no1/singer.shtml

Sleeth, C. E. (2002). Technology Map: Pervasive Computing. Menlo Park, Croyden and Tokyo: SRI Consulting Business Intelligence.

Streitz, N. A.; Geißler, J.; Holmer, T. et al. (1999): i-LAND: An interactive Landscape for Creativity and Innovation. In: ACM Conference on Human Factors in Computing Systems, Pittsburgh, Pennsylvania, U.S.A., May 15-20, 1999, New York: ACM Press, pp. 120-127.

Stross, R. (2005): Whoops! We Seem to Have Misplaced Your Identity. In: New York Times, 8 May 2005.

Subirana, B.; Bain, M. (2005): Legal Programming: Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond. New York: Springer.

Tafazolli R., Correia L. M., Saarnio J. (2005): eMobility Strategic Research Agenda. Staying ahead! eMobility Strategic Research Agenda. Mobile Communications & Technology Platform. http://www.emobility.eu.org/documents/ SRA_2005_03_18.pdf

Thomas, G.; Wyatt, S. (1999): Shaping Cyberspace: Interpreting and transforming the Internet. In: Research Policy 28, No. 7, pp. 681-698.

Tobe, Y.; Suzuki, T. (2005): WISER: Cooperative Sensing Using Mobile Robots. In: HWISE-2005, July 2005, Fukuoka, Japan. http://www.unl.im.dendai.ac.jp/%7Eyoshito/HWISE2005.pdf

Van Laerhoven, K.; Lo, B. P. L.; Ng, J. W. P. et al. (2004): Medical Healthcare Monitoring with Wearable and Implantable Sensors. In: UbiHealth 2004 - The 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications.

Varney, C.; Cole, P.; Duserick, W. et al. (2003). Privacy and Security Best Practices (Version 2.0). Liberty Alliance Project. http://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf.

Vildjiounaite, E.; Malm, E.-J.; Kaartinen, J.; Alahuhta, P. (2003): Context Awareness of Everyday Objects in a Household. In: Aarts, E.; Collier, R. et al. (Eds.): Ambient Intelligence: Proceedings of the First European Symposium, EUSAI 2003, Veldhoven, The Netherlands, November 3-4, 2003. Heidelberg, Berlin: Springer (Lecture Notes in Computer Science, 2875), pp. 177 - 191.

Wactlar, H. D.; Christel, M.; Hauptmann, A. et al. (2004): Infrastructure for Machine Understanding of Video Observations in Skilled Care Facilities - Implications of Early Results from CareMedia Case Studies. In: UbiHealth 2004 - The 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Nottingham, 7 September 2004.

Ward, V. (2004). Coming everywhere near you: RFID. IBM Financial Services. http://www-1.ibm.com/industries/financialservices/doc/content/landing/884118103.html.

Wearden, G. (2005): Labour peer bangs cyberterrorism drum. In: ZDNet UK, 27 April 2005.

Weis, S. A.; Sarma, S. E.; Rivest, R. L.; Engels, D. W. (2004): Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter, D.; Müller, G. et al. (Eds.): Security in pervasive computing: First International Conference, Boppard, Germany, March 12-14, 2003. Berlin and New York: Springer (Lecture notes in computer science, 2802), pp. 201-212.

Weiser, M. (1991): The Computer for the 21st Century. In: Scientific American 265, No. 3, pp. 94-104.

Weiser, M. (1993): Some Computer Science Issues in Ubiquitous Computing. In: Communications of the ACM 36, No. 7, pp. 75-85.

Welen, P.; Wilson, A.; Nixon, P. (2003). Scenario Analysis. Gloss Deliverable D.9. Glasgow: University of Strathclyde. http://iihm.imag.fr/projects/Gloss/Deliverables/D9-1.pdf.

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

Winters, N. (2004): Personal Privacy and Popular Ubiquitous Technology. In: Proceedings of Ubiconf 2004, April 19th, Gresham College, London.

WWRF (2001). The Book of Visions 2001: Visions of the Wireless World. Version 1.0. Wireless World Research Forum. http://www.wireless-world-research.org/general_info/BoV2001-final.pdf.

Legal Documents

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). In: Official Journal of the European Communities L 178, 17 July 2000, pp. 1-16.

Directive 2001/29 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. In: Official Journal of the European Communities L 167, 22 June 2001, pp. 10-19.

Directive 95/46/EC: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data. In: Official Journal of the European Communities L 281, 23 November 1995, pp. 31-50.

Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access. In: Official Journal of the European Communities L 320, 28 November1998, pp. 54-57.

Directive2002/21/EC: Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). In: Official Journal of the European Communities 45 L108, pp. 33-50.

Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981, *European Treaty Series*, no. 108; *International Legal Materials*, 1981, I, 422.

Treaty on European Union (consolidated text), In: Official Journal of European Communities C 325, 24 December 2002.

Treaty establishing the European Community, (consolidated text). In: Official Journal of European Communities C 325, 24 December 2002.

European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome 4 November 1950.

Protocol No 12 to the European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 4 November 2000.

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). In: Official Journal of European Communities L 108 , 24 April 2002 pp. 51 – 77.

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. In: Official Journal of the European Communities L 210, 07 August 1985, pp. 29-33.

Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices. In: Official Journal of the European Communities L 189, 20 July1990, pp. 17-36.

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs. In: Official Journal of the European Communities L 122, 17 May 1991, pp. 42-46.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. In: Official Journal of the European Communities L 095, 21 April 1993, pp. 29-34.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. In: Official Journal of the European Communities L 77, 27 March 1996, pp. 20-28.

Commission Directive 97/6/EC of 30 January 1997 amending Council Directive 70/524/EEC concerning additives in feedingstuffs (Text with EEA relevance). In: Official Journal of the European Communities L 035, 05 Februari 1997, pp. 11-13

Recommendation 3/97 on Anonymity on the Internet, Adopted by the Working Party on 3 December 1997.

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. In: Official Journal of the European Communities L 144, 04 June 1997, pp. 19-27.

Opinion 1/98 on Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), Adopted by the Working Party on 16 June 1998.

Directive 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services. In: Official Journal of the European Communities L 204, 21 July1998, pp. 37-48.

Directive 1999/93 of 13 December 1999 on a Community framework for electronic signatures. In: Official Journal of the European Communities L 013, 19 January 2000, pp. 12-20.

2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland. In: Official Journal of the European Communities L 215, 25 August 2000, pp. 1-3.

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. In: Official Journal of the European Communities L 215, 25 August 2000, pp. 7-47.

Charter of Fundamental Rights of 7 December 2000 of the European Union. In: Official Journal of the European Communities C 364.

Regulation 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. In: Official Journal of the European Communities L 012, 16 January 2001, pp. 1-23.

2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 1539). In: Official Journal of the European Communities L 181, 04 July 2001, pp. 19-31.

Commission Decision 2002/2/EC of 20.12.2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act. In: Official Journal of the European Communities L 2/13, 04 January 2002, pp. 13-16.

Directive 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. (2002): In: Official Journal of the European Communities L 201, 31 July 2002, pp. 37-47.

Commission Decision C(2003) 1731 of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina. In: Official Journal of the European Communities L 168, 5 July 2003.

Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. In: Official Journal of the European Communities L 385, 29 December 2004, pp. 1-6.

Annexes

Annex I: AmI projects

SWAMI has reviewed the following list of projects. European projects are sponsored by the European Commission unless otherwise noted. The table below has a number of gaps, which we aim to eliminate as the SWAMI project progresses.

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
EUROPE					
2WEAR	2001-2003	€3.67 m		4	http://2wear.ics.forth.gr
ACCORD	2001-2003	€1.76 m		3	Administering Connected Co-Operative Residential Domains www.sics.se/accord
ACIP	2002-2003	€400,000		13	Analysis & Assessment for Critical Infrastructure Protection www.eu-acip.de
AMBIENT AGORAS	2001-2003	€3.28 m		4	Dynamic Information Clouds in a Hybrid World www.ambient-agoras.org
AMIGO	2004-2008	€ 24 m		17	Ambient intelligence for the networked home environment www.hitech-projects.com/euprojects/amigo
AMSD	2002-2003	€399,979		6	Accompanying Measure System Dependability https://rami.jrc.it/roadmaps/amsd
ARTEMIS	2004-		industry		Advanced Research and Development on Embedded Intelligent Systems

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
					www.cordis.lu/ist/artemis
ARTEMIS			Netherlands		ARchitectures and meThods for Embedded MedIa Systems www.onderzoekinformatie.nl/en/oi/nod/onderzoek/OND1277482
ARTIST	2002-2005	€3.88 m		29	Roadmap re Hard Real Time (HRT) embedded systems www.artist-embedded.org
ARTIST2	2004-2008				Network of Excellence www.artist-embedded.org/FP6/Overview
ASSERT	2004-2007	€14.99 m		29	Automated proof based System and Software Engineering for Real-Time Applications www.mayeticvillage.com/assert
BASIS	2003-2007	€740,000	Senter Novem (Neth.)	3	biometric authentication for securing access to information and services www.sas.el.utwente.nl/home/basis
BETSY	2004-2007	€4.43 m		8	BEing on Time Saves energy www.hitech-projects.com/euprojects/betsy/index.htm
BIOVISION	2002-2003	€399,991		9	www.eubiometricforum.com
BITE	2004-			9	biometrics identification technology ethics www.biteproject.org
CEmACS	2004-2007	€2.28 m		5	Complex Embedded Automotive Control Systems www.hamilton.ie/cemacs
CoBIs		€4.73 m		7	Collaborative Business Items

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
					www.cobis-online.de
COMPARE	2004-2006	€3.43 m		6	COMPonent Approach for Real-time and Embedded www.ist-compare.org
COSINE	2005-2007	€300,000		11	Co-ordinating Strategic Initiatives on Embedded Systems in the European Research Area http://cosine.eutema.com
DECOS	2004-2007				Dependable Embedded Components and Systems www.decos.at
DELIS	2004-2007	€6.93		18	Dynamically Evolving, Large Scale Information Systems http://delis.upb.de
ECAGENTS	2004-2007	€7.12 m		10	Embodied and Communicating Agents http://ecagents.istc.cnr.it
ECRYPT	2004-				Network of Excellence on cryptology www.ecrypt.eu.org
eEPOCH	2002-2004	€4.97 m		16	eEurope Smart Card Charter proof of concept and holistic solution www.eepoch.net
eGadgets	2001-2003	€1.71 m		3	Extrovert Gadgets www.extrovert-gadgets.net
EMBEDDED WISENTS	2004-2006	€1.41 m		12	Co-operating Embedded Systems for Exploration and Control featuring Wireless Sensor Networks www.embedded-wisents.org

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
eMobility	2004-		industry		www.emobility.eu.org
EMTECH	2004-2006	€499,942		7	Embedded Systems TECHnologies www.emtech-sme.org/emtech/index2.html
EQUATOR	2000-2006	£12 m	UK EPSRC		Interdisciplinary Research Collaboration (IRC) -- technical, social and design issues in the development of new inter-relationships between the physical and digital worlds www.equator.ac.uk
EUAIN	2004-2007	€977,824		10	European Accessible Information Network www.euain.org/modules/wfsection
EUCLID	2002-2003	€674,337		4	European initiative for a Citizen digital ID solution www.electronic-identity.org
EVERGROW	2004-2008	€7.45 m		28	Ever-growing global scale-free networks, their provisioning, repair and unique functions www.evergrow.org/page.php?id=1
FEEL	2001-2003				Non-Intrusive Services to Support Focussed, Efficient and Enjoyable Local Activities
FiCom	2001-2003	€3.55 m		4	Fibre Computing www.fibercomputing.net
FIDIS	2004-2009	€6.1 m		24	Future of Identity in the Information Society www.fidis.net
FLAGS	2002-2004	€1.53 m		5	Foundational Aspects of Global Computing

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
GLOSS	2001-2003	€1.74 m		4	Global Smart Spaces www.gloss.cis.strath.ac.uk/index.html http://iihm.imag.fr/projects/Gloss/
GOLLUM	2004-2006	€3.01 m		7	Generic Open Link-Layer API for Unified Media Access www.ist-gollum.org
GROCER	2001-2004	€2.23 m		3	Grocery Store Commerce Electronic Resource www.cordis.lu/ist/fet/dc-sy.htm
GUIDE	2004-2005	€12.47 m		23	Government User IDentity for Europe http://istrg.som.surrey.ac.uk/projects/guide
HIJA	2004-2006	€3.99 m		13	High-Integrity Java Application www.hija.info
HiPEAC	2004-2008	€21.8 m		16	High-Performance Embedded Architectures and Compilers http://escher.elis.ugent.be/hipeac
HYCON	2004-2008	€4.6 m		23	Network of Excellence -- Hybrid Control www.ist-hycon.org
ICODES	2004-2007	€4.44 m		7	Interface and Communication based Design of Embedded Systems http://icodes.offis.de
INTERLIVING	2001-2003	€1.81 m		3	Designing Interactive, Intergenerational Interfaces for Living Together http://interliving.kth.se
ITEA	1999-		industry		Technology Roadmap on Software-Intensive Systems

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
	2008				www.itea-office.org
MEDEA+			industry		Applications Technology Roadmap (ATRM) www.medea.org/webpublic/publications/publ_atrm.htm
MiME	2001-2002	€738,479		3	Multiple Intimate Media Environments www.mimeproject.org
MOSAIC	2004-2005	€1.24 m		15	Mobile Worker Support Environments: Aligning Innovation in Mobile Technologies, Applications and Workplaces for Location-Independent Co-operation and Networking
NeCST	2004-2007	€1.72 m		7	Networked Control Systems Tolerant to faults www.strep-necst.org
ORESTEIA	2001-2003	€2.61 m		6	Modular Hybrid Artefacts with Adaptive Functionality www.image.ntua.gr/oresteia
OZONE	2001-2004	€12.21 m		9	New technologies and services for emerging nomadic societies www.extra.research.philips.com/euprojects/ozone See also www.hitech-projects.com/euprojects/ozone
PALCOM	2004-2007	€11.14 m		12	Palpable Computing www.ist-palcom.org
PAMPAS	2002-2003	€633,442		7	Pioneering Advanced Mobile Privacy And Security www.pampas.eu.org
PAPER++	2001-2003	€1.52 m		5	www.paperplusplus.net
PAW	2003-		IOP GenCom	4	Privacy in an Ambient World

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
	2007		Senter (Neth.)		www.cs.ru.nl/~jhh/paw/index2.html
PISA	2001-2004	€3.2 m		9	Privacy Incorporated Software Agent www.pet-pisa.nl/pisa_org/pisa/index.html
PRIME	2004-2008	€13.14 m		21	Privacy and Identity Management for Europe www.prime-project.eu.org
PROFIT			Eurescom		Potential pRofit Opportunities in the Future ambient InTelligence world www.eurescom.de/public/projects/P1300-series/ p1302/P1302_portal.asp#P1302%20Deliverable%201
PROGRESS			Technology Foundation STW		Embedded Systems Roadmap 2002
RAPID	2002-2003	€399,134		8	Roadmap for Advanced Research in Privacy and Identity Management https://rami.jrc.it/roadmaps/rapid/overall.pdf
RUFAE		€500,000 +	universities		Research on User-Friendly Augmented Environments 10 research groups in the US and Europe who are sharing their HCI findings www.rufae.net http://media.informatik.rwth-aachen.de/msp.html
RUNES	2004-2007	€10.72 m		22	Reconfigurable Ubiquitous Networked Embedded Systems
SHAPE	2001-	€1.92 m		4	Situating Hybrid Assemblies in Public Environments

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
	2004				www.shape-dc.org
SMART-ITS	2001-2003	€2.67 m		5	Interconnected Embedded Technology for Smart Artefacts with Collective Awareness www.smart-its.org
SOB		€734,000		4	Sounding Object www.soundobject.org
STORK	2002-2003	€200,000		8	Strategic Roadmap for Cryptology www.stork.eu.org
TECAP	2004-2005		Academy of Finland		Tools for Energy Consumption Aware Processing
UCC			Stockholm University & KTH		ubiquitous computing and communication Future Ubiquitous Service Environments (FUSE) http://dsv.su.se/fuse/
WEARIT@WORK	2004-2008				www.wearitatwork.com
Wireless physiological sensors	2003-2006	€780,000	Academy of Finland		Wireless physiological sensors for ambulatory and implantable applications www.ele.tut.fi/tule
WorkSPACE	2001-2003	€1.52 m		6	Distributed Work support through component based SPAtial Computing Environments www.daimi.au.dk/workspace/index.htm
WWRF	2001-		industry		Wireless World Research Forum www.wireless-world-research.org

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
			UNITED STATES		
AURA	2000 -		DARPA	Carnegie Mellon University	personal information aura www-2.cs.cmu.edu/~aura
Aware Home Research Initiative (AHRI)	2000 -	$700,000 +	NSF, industry	Georgia Institute of Technology,	In addition to the $700,000 grant from the Georgia Research Alliance, the project received funding from more than 20 companies and the NSF. www.awarehome.gatech.edu
CENS	2002-2012	$40 m	NSF	UCLA	Center for Embedded Networked Sensing www.cens.ucla.edu
CHESS	2002 - 2007	$13 m	NSF	University of California at Berkeley	Center for Hybrid and Embedded Software Systems Seeks to provide new engineering methods for the design of complex embedded systems that are reliable and robust to partial system failures. Other partners are the Institute for Software Integrated Systems at Vanderbilt and the Department of Mathematical Sciences at the University of Memphis. http://chess.eecs.berkeley.edu/
CLEVER			NSF		Cognitive Lever http://l3d.cs.colorado.edu/clever
DETER	2003-06	$10.8 million	NSF and the Department of Homeland Security	University of California-Berkeley	cyber Defense Technology Experimental Research network Other partners include the University of California Davis, University of Southern California-Information Systems Institute, Network Associates Laboratories, SRI, Menlo Park, Pennsylvania State University, Purdue University, Princeton University, University of Utah, and industrial partners Juniper Networks, CISCO, Intel, IBM,

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
					Microsoft, and HP. www.isi.edu/deter
MANTIS	2002 -		NSF	University of Colorado at Boulder	MultimodAl NeTworks of In-situ Sensors Wireless sensor networking http://mantis.cs.colorado.edu
Margaret			IBM	IBM	Technologies to protect privacy www-1.ibm.com/industries/financialservices/doc/content/landing/884118103.html
MIThril	2000 -		MIT Media Lab	MIT Media Lab	next-generation wearables research platform www.media.mit.edu/wearables/mithril/overview.html
MoBIES	2000 - 2003		DARPA		Model-Based Integration of Embedded Software technology for systematic composition of embedded software components
NEST	three years	$2.1 m	DARPA	University of California at Berkeley	Network Embedded Systems Technology http://webs.cs.berkeley.edu/nest-index.html
Oxygen	2000 - 2005	$50 million	DARPA and industry	MIT	Sponsored by Acer and Delta Electronics, Inc. (Taiwan), Hewlett-Packard Corp. (USA), NTT (Japan), Nokia Research Center (Finland), Philips Research (Netherlands) http://oxygen.lcs.mit.edu/index.html /www.oxygen.lcs.mit.edu/Overview.html
PeopleVision			IBM	IBM	Smart Surveillance Engine

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
					www-1.ibm.com/solutions/businesssolutions/doc/content/solution/972941107.html
Planet Blue	2000 - 2004?	$180 million	IBM	IBM	how people will interact with the emerging world of the wireless Internet www.research.ibm.com/compsci/planetblue.html
PORTIA	five-year		NSF	Yale and Stanford	Privacy, Obligations, and Rights in Technologies of Information Assessment A multi-institutional, multi-disciplinary, multi-modal investigation that looks comprehensively at sensitive data in a networked world. http://crypto.stanford.edu/portia
Portolano			DARPA	University of Washington	Reconfigurable computing. http://portolano.cs.washington.edu
RoSES	2001 -		General Motors	Carnegie Mellon University	Robust Self-configuring Embedded Systems. Other partners and/or sponsors include: Bosch, Pennsylvania Infrastructure Technology Alliance, ADtranz, Intel, Lucent, U.S. Air Force, NSF , DoD, TTTech www.ece.cmu.edu/~koopman/roses
SCADDS	1999 - 2003		DARPA NSF	USC/ISI	ScalableCoordination Architectures for Deeply Distributed Systems www.isi.edu/scadds
SHARP	2001 -		Intel	University of Washington	System for Human Activity Recognition and Prediction www.intel.com/research/areas.htm

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
Smart Dust	1997-2001			University of California at Berkeley	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. http://robotics.eecs.berkeley.edu/~pister/SmartDust
Smart Matter	late 1990s		PARC, a subsidiary of Xerox	PARC, a subsidiary of Xerox	Development and integration of sensors, actuators and computational elements requiring intelligence, control and reconfiguration http://www2.parc.com/spl/projects/smart-matter/
Software Enabled Control (SEC)	1999 – 2002?			University of California at Berkeley	Hybrid System Design Tools for Software-Enabled Control http://sec.eecs.berkeley.edu/
SPARCLE	2003 -		IBM	IBM, Univ of Maryland	Server Privacy ARrchitecture and CapabiLity Enablement Enabling privacy policies www.research.ibm.com/privacy
Tiny OS	2000 -			UC Berkeley	TinyOS is an open-source operating system designed for wireless embedded sensor networks. Over 500 research groups and companies are using TinyOS on the Berkeley/Crossbow Motes. http://tinyos.millennium.berkeley.edu www.tinyos.net
TRUST	2005 -	$19 million	National Science Foundation	University of California at	Team for Research in Ubiquitous Secure Technology nine universities and 11 big companies, including Bellsouth, Cisco, HP, IBM, Intel, Microsoft, Sun, and ESCHER (a research

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
				Berkeley	consortium which includes Boeing, General Motors and Raytheon www.nsf.gov/news/news_summ.jsp?cntn_id=103178& org=NSF&from=news
JAPAN[155]					
21st Century COE	2002 -		MEXT	Keio University	Ubiquitous middleware for smart computing environment and their applications to social issues. www.coe21.sfc.keio.ac.jp/eng/index.html
CRUISE/r				Tokyo Denki University	Ubiquitous personal lost and found system for public transportation passengers. www.unl.im.dendai.ac.jp/wiser
Micro Hot Spots				Keio University	Converting non-smart space into a “smart hot-spot”. www.ht.sfc.keio.ac.jp/mhsn
Next Generation Mobile Network	2002 -		NICT	industry, universities	Development of new technologies to enable seamless and secure integration of various wireless access networks such as 3G and 4G cellular, wireless LAN, Bluetooth, ultra-wideband, fixed wireless access and intelligent transport system. In collaboration with industries and universities, the Yokosuka Radio Communications Research Center of the National Institute of Information and Communications Technology (NICT) created a test bed for evaluating new technologies. www2.nict.go.jp/mt/b190/e/outline/outline.html

[155] In addition to the projects listed here, many more can be found on the websites of the ubiquitous networking research laboratories referenced in Chapter 3, section 3.3.4.

Project acronym	start / finish	budget	sponsor	partners	project title, theme / issues & websites
STONE	1999 -			University of Tokyo	Innovative network architecture for supporting future ubiquitous computing applications. STONE provides service discovery, context awareness, service synthesis, and service mobility. www.mlab.t.u-tokyo.ac.jp/research
Ubila			MIC	industry, academia	Control management technologies for ubiquitous networks. Participants include the University of Tokyo, Kyushu Institute of Techology, NEC Corporation, Fujitsu Limited, KDDI R&D Laboratories Inc., KDDI Corporation. www.ubila.org
UbiLab				Keio University	Ubiquitous Computing Laboratory (UbiLab) develops fundamental and application software. It has created Smart Furniture, which can be placed within an area with no network connectivity so that it becomes a Smart Space, with network connectivity and services. UbiLab members include people from Keio University, Tokyo Denki University and the Tokyo Institute of Technology
WISER				Tokyo Denki University	Ad hoc communication architecture for multiple nodes ("mobile robots") www.unl.im.dendai.ac.jp/wiser
Yaoyorozu	2002 - 2005		MEXT	Hitachi, U. of Tokyo, Keio U, the Nat'l Inst. of Media Education Tokyo U of Tech, UDIT	"Research on Ubiquitous Information Society based on Trans-Disciplinary Science" Desirable institutional systems and core technology for the ubiquitous information society in 2010. www.8mg.jp/en/outline_goals01.htm

Annex II: Framework for scenario analysis

The following dimensions have been used to analyse the contents of existing Ambient Intelligence Scenarios

Actors in the scenario

Some scenarios are targeted at a certain category of actors (people), e.g. salespersons or single young people who want to find a friend; or scenarios can be targeted at helping elderly or disabled persons. Other scenarios cover relatively wide range of normally working people. From the point of view of acceptance of new technologies, some scenarios assume that most of people have accepted AmI, while other scenarios are targeted at people who are ready to accept new technology at early stages. Due to having different target groups in the scenario, actors in the scenario are described by their age group, health group, profession, social status and attitude towards technology. This dimension is important because social, legal and privacy issues depend on scenario actors, e.g. people with severe disabilities can be willing to exchange some privacy to get more support, and small children don't care much about privacy. On the other hand, politicians usually care much more about personal data than average people.

Actors in the scenario				
age	health	profession	social status	early technology acceptance
No special target Children Teenagers Young Working age Elderly	No special target People with severe disabilities People with mild disabilities Sportsmen	No special target Business Politicians Journalists ...	No special target Married Having children Single	No special target Technology enthusiasts

Environment where the scenario takes place

The following environmental descriptors were used to analyse the scenarios: urban, long-distance travelling, country-side and nature. This dimension is important because in different environments different technologies are needed, and because it shows where changes can appear earlier. The dimension is also important because people have different expectations about privacy in different environments, e.g. in their own home and in the nature people are less willing to accept same behaviour restrictions as in public places.

Environment where the scenario takes place
Urban
Long-distance travelling
Country-side
Nature
At home

Activity described in the scenario

The following descriptors were used to analyse the activities in the scenarios: work, learning, ordinary everyday activities like household-related activities, changing places, leisure and hobby, social, health maintenance, emergency. This dimension is important because information flow is closely linked to the activity, and main privacy threats are related to information flow.

Activity described in the scenario
Work
Everyday, housekeeping
Changing places
Hobby, leisure
Social
Emergency
Health maintenance
Learning

AmI control level vs. person control level

Different scenarios assume different level of AmI control. Some scenarios assume that AmI acts on behalf of the person without disturbing a person (e.g. AmI checks a bill and pays it without notifying the user that the transaction took place, or AmI lowers car speed for accident avoidance or environmental reasons). In other cases AmI only provides information to humans and gives advices, leaving the decision to a human. Situations when AmI only executes persons' commands without providing to a person some kind of information proactively are not often described in AmI scenarios, but they definitely exist. This dimension is important because it raises a lot of questions about legal responsibility (when AmI makes the decision, who is legally responsible for it?), and because it affects humans' acceptance of AmI.

AmI control level vs. person control level
High: AmI acts on behalf of the person
Medium: AmI gives advices
Low: AmI executes person's commands

Information flow in the scenario

Since most of privacy threats are associated with disclosure of information, we suggest to categorise scenarios by how much AmI needs to know about people, organisations and objects in order to realise the scenario, namely, does AmI use highly sensitive personal data, data of medium sensitivity or low sensitivity. It is also important to differentiate between information storage and information exchange because it implies different means and times of information access. However, it is rarely explicitly mentioned in the scenarios where information is stored (e.g. in the infrastructure or in a personal device). Information exchange depends on the implementation of information storage. Thus, if information storage is not explicitly described in scenarios, in scenario analysis we assume that most of personal data is stored in a personal device because it is safer from the privacy point of view.

Information flow in the scenario			
Personal Data	Organisations data	Environmental data	Objects data
High sensitivity • Personal Identity data • Personal financial data for paying bills Medium sensitivity • Personal location • Personal health • Personal professional data Low sensitivity • Personal preferences	High sensitivity • Intellectual property data • Organisation financial data for paying bills Medium sensitivity • Organisation events • Low sensitivity • Organisations contact information • Organisation financial data for receiving payment		Location Description

- Personal contact information - Personal financial data for receiving payment			

Enabling Technologies

ISTAG has identified ten Key Enabling Technologies for AmI. We use a less detailed categorisation of Enabling Technologies, namely, four major groups: Embedded Intelligence, Communications, Interfaces and Sensors, and we suggest to categorise them by how advanced they need to become compare with the current situation. We suggest using of only two grades: Highly Advanced and More Realistic (or Not So Advanced), meaning that Not So Advanced Technology allows scenario implementation without the need in radical changes to existing technologies, even if radical changes might be needed to increase security or privacy. For example, personal identification can be implemented with the help of electronic ID cards, passwords and biometrics, which is fairly realistic, but not unobtrusive. Personal identification can be also implemented in a more secure way with the help of implants, and this way will work much faster. However, if it is not explicitly stated in the scenario, we assume implementation of a More Realistic way first. Similarly, if the scenario can be implemented by giving command "emergency call!" to a system, we don't require AmI to be able to conclude that the user is now in emergency situation because a maniac is chasing her.

Enabling Technology			
Communications	Interfaces	Sensors and actuators	Embedded Intelligence
Highly Advanced - high density of communicative objects - large numbers of communicative objects - seamless interactions between different networks	Highly Advanced - natural multimodal interfaces - emotion recognition Not So Advanced - limited number of gestures	Highly Advanced - high precision face recognition - unobtrusive emotion recognition - unobtrusive person identification	Highly Advanced - detection of high-level contexts and choice of appropriate actions - high-level reliable personalisation - automatic resolving of ambiguities Not So Advanced - detection of simple contexts

Not So Advanced • wired communication • peer-to-peer communication • communication within one network	• limited number of voice commands	Not So Advanced • fingerprint • smoke detection • gas analysis	• simple personalisation • involving a user in case of ambiguity or uncertainty

Threats associated with information losses in the scenario

This part of the scenario analysis has been most speculative, because threats are usually not explicitly described in the scenarios, and because it is impossible to predict how certain type of information can be used with malicious intentions. Moreover, privacy is culture-dependent and person-dependent construct.

Thus, we have categorised possible threats roughly in a following way: High: an information loss can be potentially dangerous for lives of people (knowing person location and route makes kidnapping or killing of a person easier); Medium: for people health or well being (e.g. financial fraud); Low: mainly for a personal comfort (e.g. family conflict due to disagreement on how to spend money).

Threats which can appear in the scenario		
High risk	Medium risk	Low risk
Life of a person	Health	Personal discomfort
Life of a beloved person	Finances	Advertisements spam

Alternative ways of problem solving

The last issue is the trade-off between privacy threats and benefits which people could get from scenario realisation. If the problem, described in the scenario, can be solved by other means than suggested in the scenario, and these means are less privacy-threatening, the next step would be to evaluate the competitive ways from economical point of view and acceptability point of view, which is beyond the scope of this paper. However, we think that it is very important to point out alternative ways to problem solving if they exist. Although this part of the scenario analysis is speculative to some extent, we suggest including it to scenario analysis, and not because we are against developing of security means. For the sake of privacy we suggest application of security and encryption methods to all personal data flow, but it is always safer not to create at all, if possible, the situation where security and encryption algorithms are needed.

Alternative technological ways to problem solving as they might be found (human recourses are not considered as alternative means):

- Implementation of another functionality instead (e.g. building of another kind of infrastructure than the one described in the scenario)
- Implementation of same functionality by different means (e.g. anonymous cards for payment instead of personal ones).

Annex III: Opinions and documents of Article 29 Working Party

This list contains the most important opinions and documents of the Art.29 Working Party on issues of privacy, identity and security.

Data Protection Directive 95/46 set up a Working Party on the Protection of Individuals with regard to the Processing of Personal Data, called Article 29 Working Party (WP). The WP has an important *advisory status*.

It advises the Commission on any proposed amendment of the directive on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed EC measures affecting such rights and freedoms. It also can give opinions on codes of conduct drawn up at Community level and make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

This full text of these documents and opinions can be consulted on the website of WP 29, i.e. *http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm*

1997:

Recommendation 3/97 on Anonymity on the Internet

1998:

Opinion 1/98 on Platform for Privacy Preferences and Open profiling Standard

2002:

Working Document on the surveillance of electronic communications in the workplace

Working Document on application EU data protection law to non-EU based websites Opinion 1/2002 on the CEN/ISSS Report on Privacy Standardisation in Europe

Working Document on Blacklists

Working Document - First orientations concerning on-line authentication services

2003:

Working Document on Biometrics

Opinion 2/2003 on the application of data protection principles to Who is Directories

Opinion 7/2003 on re-use of public sector information and protection of personal data

2004:

Opinion 9/2004 on the Draft framework Decision of 28 April 2004 on Data Retention

Opinion on More Harmonized Information Provisions

Declaration of the Article 29 Working Party on Enforcement

Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance

2005:

Working Document on data protection issues related to Intellectual Property Rights

Working document on data protection issues related to RFID technology

Deliverable Summary Sheet

Project Number:	IST-2004-006507
Project Acronym:	SWAMI
Project title:	Safeguards in a World of Ambient Intelligence
Deliverable no.:	1
Due date:	June 2005
Delivery date:	Draft version, July 2005 Revised version, January 2006
Delivery status:	Public
Work package no.:	1
Leading partner:	Fraunhofer Institute for Systems and Innovation Research (project co-ordinator), Technical Research Center of Finland, VTT Electronics (Work Package Leader)
Contributing partners:	All
Partners owing:	All
Distribution Type:	Public