Safeguards in a World of Ambient Intelligence (SWAMI): Scenario Analysis and Legal Framework – First Results

Report submitted to the participants of the first
SWAMI expert workshop, held in Brussels, 1 June 2005

Michael Friedewald, David Wright, Elenena Vildjiounaite
(editors)

Contributors: Elena Vildjiounaite, Petteri Alahuhta (VTT Electronics); Yves Punie, Sabine Delaitre, Ioannis Maghiros (JRC-IPTS); Michael Friedewald (Fraunhofer ISI); Serge Gutwirth, Wim Schreurs, Michiel Verlinden (Vrije Universiteit Brussel); David Wright (Trilateral Research & Consulting)

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

About SWAMI:

The SWAMI project aims to identify and analyse social, legal, organisational and ethical implications related to issues such as privacy, anonymity, manipulation and control, and identity in the context of Ambient Intelligence (AmI) using current and future information and communications technologies.

The first step was a review of existing AmI projects, studies, scenarios and roadmaps to ensure that the SWAMI project captures, as far as possible, the major trends and issues.

As a second step the consortium will 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.

Finally we will define and study various research and policy options, which could serve as safeguards and privacy-enhancing mechanisms that address the risks and vulnerabilities identified before. The aim will be to identify mechanisms, which will ensure user control, user acceptance and enforceability of policy in an accessible manner, as well as to ensure that all Europeans have real equal rights and opportunities of accessibility to the Ambient Intelligence space.

Website: http://swami.jrc.es

Contents

1 Introduction 4

2 Aspects of privacy 4

3 Constructing scenarios 5

4 Future visions 7

5 Scenario dimensions 13

6 Enabling technology 18

7 Threats in a World of Ambient Intelligence 24

8 The existing legal framework for AmI 28

1 Introduction

This work presents an analysis of the privacy and social implications of using ambient intelligence (AmI) technologies in everyday life in the not very distant future. For this analysis, the SWAMI partners reviewed more than 70 projects and roadmaps, many of which have scenarios. We also reviewed more than 60 other research publications to have a better understanding of where the joint efforts of AmI researchers are leading and of how AmI is likely to change our lives. The AmI vision of everyday life in the foreseeable future is a mixture of many diverse applications ranging from relatively-easy-to-realise prototypes to scenarios in the more distant future taken from roadmaps. We have clustered the many aspects of our future everyday lives in the following application domains: home, work, learning, health, shopping and mobility.

This paper is structured as follows: first, we present views of several researchers on privacy and its aspects. We then explain how we synthesised an 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, their visions, and the specifics of their visions. After that, we list the main benefits, threats and open issues identified in the scenarios, and finally we present our conclusions together with a brief analysis of the legal framework applicable to AmI.

2 Aspects of privacy

Bohn et al. (2005) argue that there are different dimensions related to privacy and new technologies, in particular Information and Communication Technology (ICT). The following aspects of privacy are identified:

Privacy as empowerment. Privacy has an informational aspect. People should have 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.

Furthermore, Bohn et al. (2005) draw upon Gary Marx (2001) to describe that people perceive their privacy being invaded when borders are crossed. The following borders are identified: *Natural borders*. Observable physical borders, such as walls and doors, clothing, darkness,

sealed letters and phone conversations, and 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 include, for example, 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. Most people expect 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 authors develop these aspects of privacy. 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 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 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 may be 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, Singers work also links privacy to personal development.

3 Constructing scenarios

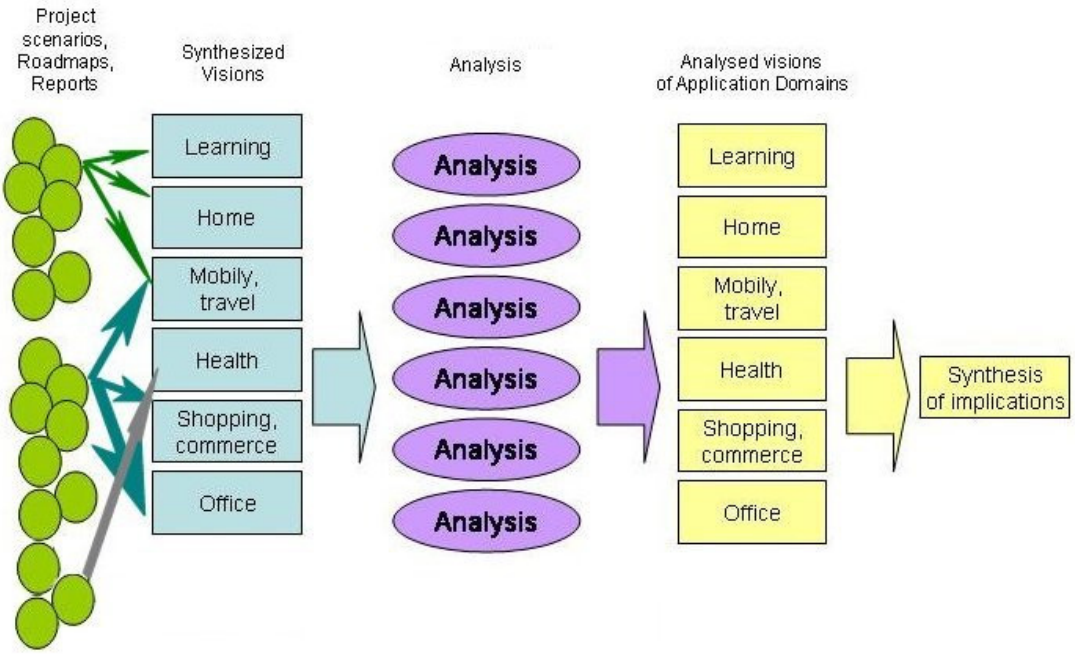
Constructing scenarios is a way to present in a concise form the most visible research activities in a certain application domain. AmI application scenarios can be found in many different forms.

- First, there are *elaborated scenarios* (screenplays) with actors and their activities, with many details and a well-defined storyline. These scenarios can be either purely conceptual, theoretical visions of a future (good examples are the ISTAG scenarios) 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 are not scenarios in the strict sense. They do not present any storylines but rather describe situations and/or drivers or trends that may give rise to relevant AmI applications. (See, for instance, Michahelles 2003 on how technology helping to save lives of avalanche victims when skiing.) 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.

The following graph summarises different approaches to research and visions on AmI:



The SWAMI partners have synthesised and analysed the available material on AmI. The synthesis is not presented as a scenario storyline, but as a list of people's activities supported by AmI. It provides a structured and easy to grasp view. A more detailed analysis than that presented here in summary form can be found in the SWAMI project deliverable [D1].

For its synthesis of visions and scenarios from numerous sources, SWAMI developed the following analytical framework:

- available information about the personality of the main *actor*, 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 where 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;
- the 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 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 dependability on AmI; third, affects humans' acceptance of AmI and last, raises a lot of questions about legal responsibility (when AmI makes the 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, one of the scenarios contains a statement: "The agent knows the preferences of Elena's friends since they have earlier been to Elena's place". We think that "since they have earlier been to Elena's place" is an important scenario element because it indicates that information is stored somewhere in the system.

4 Future visions

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 per-

sonal 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 which kind of information about someone can not be found in the home environment. Also, 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 (2005) said, 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:

- providing 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 are checking 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.

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.

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.

Our analysis of research projects targeted at developing AmI at work has shown that visions of 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:

- providing 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 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 semi-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.

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, especially 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 to support autonomous or semi-autonomous life and to make 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 to become possible at any place and any time, with the help of sophisticated embedded sensors and/or actuators.

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 customers 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 customer 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 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.

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 individuals own pace, promoting learning for personal, civic and social purposes as well as for employment-related purposes.

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

AmI should support the following activities:

- intentional learning, i.e., learning for a purpose by people wanting to take 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 on ones 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.

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 purposes 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 with people (friends and family);
- One kind of communication is worth being highlighted; it is about the negotiation tools. These tools allow the negotiation among agents (between personal agent and others, such as transactions agents) and will play an essential role in the mobility domain because of the possibility of acting on the move, e.g. checking a validity passport while the passenger is walking in the airport.
- 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.

5 Scenario dimensions

We consider the following dimensions as important for scenario analysis from the point of view of privacy threats and social implications. These dimensions are crucial in any application domain, as is evident from the preceding section.

Actors in scenario activities

Most of the scenarios we analysed feature ordinary working people (some are in the executive class), 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, though, an individual can have an allergy).

AmI that is 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 signals), 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 social 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 usually 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 (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. 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.

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 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 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 (lightning, 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 customers 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. However,

it begs the question about whether the emergency system would continue to function properly if 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 most clearly: the personal device assistant can even mimic his owner's speech and talk to callers on his behalf. In scenarios which describe "always on" video connection between two different 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.

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 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 objects 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 available budget, 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 central databases, but also extensive ad hoc communication. First, personal/wearable devices have to communicate with systems in the physicians 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 retailers 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.

6 Enabling technology

Ubiquitous computing

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

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

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

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

Ubiquitous computing systems 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, inter alia, 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.

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 (1999), 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.” He cites impressive examples of broken cryptographic algorithms).

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, this does not present a danger to anybody. Unfortunately, due to using unique identifiers in communication protocols[1], 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 eyeglasses (Orr 1999). Other suggested applications are usage of RFID tags in e-passports (Juels 2005), credit cards (Ward 2004) and generally everywhere (Ward 2004).

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

[1] IP addresses, MAC addresses, Bluetooth physical device ID, UIDs of RFID tags, IMEI code of mobile phones

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.

User-friendly interfaces

AmI scenarios describe highly advanced user-friendly interfaces, most popular of which are speech interfaces capable of understanding of a persons 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. 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.

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.

Also, its useful to recall that personal devices are often lost or stolen when they are already "on" (after the owner has logged on) and 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 of AmI visions is personalisation, which to large 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.

Sensors and actuators

The most common sensor features mentioned in AmI scenarios are those that provide a location-based service or positioning, biometric authentication, physiological and health condition. The most popular position determination technology outdoors is currently satellite-based, such as Global Positioning System or Galileo. 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 will lead to 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 is not mature yet. The main privacy concern in biometric applications is prevention of identity theft, i.e., using somebody elses biometric data for ones

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 persons true emotions even to a computer could be dangerous, since data protection is not perfect yet and wont 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 about 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.

Summary

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 users 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 intelligence, 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 dont know what they can do to protect themselves, or unable to cope with the technology.

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 peoples 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 a reason to trust 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."[2]

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 at the same time. 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.

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 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 retailers 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

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

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 persons 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 these unintended uses are highly undesirable (Beckwith 2003).

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).

Identity theft

Identity theft is the act of obtaining identity information without the concerned persons 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.[3]

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 purpose. How does a person discover whether he is victim of identity theft? In case of 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 a refusal for a loan application, etc.

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 unauthorized monitoring, but not alteration or destruction of data (e.g., wiretapping). 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 fires being lit.

- 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] 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.

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 abandon the activity at all. 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 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 also 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?

8 The existing legal framework for AmI

This is a summary of our overview of the existing legal framework for ambient intelligence. 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.

In the overview, we describe the applicable law and try to identify the possible AmI-related problems and challenges in connection with privacy and identity on the one hand and security on the other hand.

Since we are studying AmI from a European Union perspective, we mainly focus on European Union legislation. We only analyse international legislation when it has an impact on the European Union policies.

Privacy and data protection

Before studying privacy and data protection, the legal overview clarifies the important difference between those two legal concepts. *Article 8 of the European Convention of Human Rights* (ECHR) is analysed, since it 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. Concerning the protection of personal data, article 8 ECHR shows 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 the right of access to data on oneself is not covered. This is, of course, where data protection comes in.

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 challenge emerges because important aspects of AmI as well as its supporting technologies need to be in compliance with the principles of data protection law. AmI is being developed to provide enhanced, personalised services and to enrich our lives. This is important, because this human-centred approach indicates that the AmI system most probably needs to process substantial amounts of personal data and profiles in order to provide these services. However, 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.

A specific problem related to the *Privacy & Electronic Communications Directive 2002/58* concerns data retention. The directive stipulates that Member States may, for a limited number of reasons, enact legislation providing for the retention of traffic and location data by telecommunications operators. This data retention might, however, create important threats to data protection and privacy.

A final important issue concerning privacy and data protection is the right to anonymity on the Internet and, in the future, in an AmI world. On this point, the *Working Party 29 recommendation 3/97*[4] elaborates the dilemma between privacy and security when considering anonymity on the Internet.

An important document discussed in the overview of legal issues is the so-called Safe Harbour agreement concluded between the USA and the European Union. US firms operating under the agreement pledge to protect data from European partners in accordance with European law.

[4]The Article 29 Working Party was established as a result of Article 29 of the Data Protection directive. It comprises expert representatives from the Member States and a chairman from the European Commission. Its task is to consider and make recommendations with regard to data protection issues.

E-commerce and consumer protection law

Directive 93/13 on unfair terms in consumer contracts 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. 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. These suppliers should not be allowed to set out conditions which are manifestly not in compliance with the generally applicable privacy rules and which disadvantage the consumer. They should also not be allowed to unfairly limit their liability for security problems in the service they provide to the consumer.

The *Directive 97/7* on consumer protection in respect of distance contracts determines which information should be provided to the consumer in this context. It refers explicitly to the right to privacy and data protection, stipulates limitations to the use of unsolicited marketing and contains an article that forbids inertia selling[5]. This is important for AmI since services and communications in an AmI world will become increasingly personalised and intrusive. The provision of the necessary information as foreseen in the directive - might encounter certain problems in an AmI world.

The *e-commerce directive 2000/31* stipulates important and substantial information obligations for the services provider. It also 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. It is also regrettable that the directive does not contain rules on the liability of intermediary services providers when they violate privacy rules. The e-commerce directive obliges information service providers to stop the distribution of illegal content on their networks (the so-called notice and take-down procedure) but it is not sure whether this notice-and-take down procedure applies also to illegal content concerning personal data.

Torts and liability

In an AmI world, an increasing number of actors will be involved in the creation and provision of products. Many different producers will provide parts of the final product. When a defective product causes damages, it will be very difficult to determine which producer to hold liable for the damages caused and whether this producer has committed a fault that caused the damage. That is why 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 not apply to services and it is unclear whether it applies to software. In many cases, in an AmI world, the general rules on liability will still apply and problems remain. The directive does

[5] Inertia selling is the supply of goods or services to a consumer without their being ordered by the consumer beforehand.

not provide that a product is defective when it insufficiently protects against privacy violations or when it easily allows identity theft.

Intellectual Property Rights

Directive 91/250 harmonises the copyright protection of software within the European Union. The legal protection regime for software is of importance to the development of AmI, the implementation of standards and the achievement of interoperability. A number of exceptions are provided to allow the use of computer programs without prior authorisation. The exceptions foreseen seem to be insufficient to allow the free use of computer programs required in an AmI world. The directive allows, under certain conditions, *decompilation* of software in order to achieve the *interoperability* of an independently created computer program with other programs. Both types of exceptions are, however, limited, since the exception concerning the use of computer programs can only be invoked by the lawful acquirer and the exception for reasons of decompilation is only allowed for licensees.

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 (at the same time) for providing AmI services. It foresees a double protection for databases: a copyright protection and a *sui generis* database protection. The exceptions provided to the exclusive right of the maker of the database are rather limited and optional. In order to solve some problems concerning the use of databases, an exception to the exclusive right of the maker of the database could be created, when the use of parts of the database is necessary in order to deliver or enjoy AmI services. This is not foreseen in the directive.

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. Important for AmI is the fact that it allows under strict conditions an exception to the exclusive right of reproduction in case of temporary reproductions. It also harmonises the legal protection of effective technical measures against copyright violations. It finally stipulates that Member States have to provide for an adequate legal protection of rights-management information. Such rights-management information could, however, 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. It also provides criminals with interesting information: is the user at home or not? Is he on-line?

ICT law

Directive 1999/93 creates a legal framework for electronic signatures and for certain certification services. The general aim is to strengthen confidence in, and general acceptance of, the new technologies. The directive tries to promote the establishment of certification services providers, both by ensuring the free movement of their services and by organising their supervision by the country of establishment. Next to this supervision mechanism, the directive deals with the liability of certification service-providers and with secure signature creation devices. It finally stipulates some important principles concerning the legal effects of electronic signatures. Certified electronic signatures are important for AmI, since they might facilitate pseudonyms on the

Internet. They also might enhance the security of electronic transactions in an AmI world. The publication of generally recognised standards might solve problems of interoperability.

Other important issues concerning ICT and AmI are standards and interoperability. In the AmI scenarios, many different technologies have to work together and they need to be compatible. A way to realise this compatibility is the creation of standards. These technical standards could, however, constitute barriers to trade within the internal market. That is why *Directive 98/34/EC on technical standards and technical regulations in Information Society Services* foresees a detailed information procedure. This allows the European Commission, the Member States and the economical operators to be aware of technical standards and regulations which the Member States want to install. It should improve both the transparency and legal certainty. The information and co-operation 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. It also gives an important definition of Information Society Services.

WP 29 Opinion 1/98 describes Platform for Privacy Preferences (P3P) and Open Profiling Standard (OPS). The single vocabulary created by P3P might be 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. Creating a single vocabulary should not lead to the lowering of standards. The Open Profiling Standard should ensure the secure transmission of a standard profile of personal data.

Finally our overview of the legal framework discusses ICT implants. At this time, the use of these implants is limited to active medical devices. In an AmI world, ICT implants could be used much more frequently, such as for identification and location purposes. *Directive 90/385 on active implantable medical devices* sets out strict essential requirements which have to be fulfilled by these medical devices in order to ensure a high level of safety. The directive does not take into consideration how these devices could threaten privacy and identity. In an AmI world, implants will be used for non-medical reasons and this might require even stricter rules, since the safety risks are not counterbalanced by the positive effects on health.

The Opinion of the European Group on Ethics in Science and New Technologies on the ethical aspect of ICT implants in the human body sets out some general principles, which could be the basis for legal standards necessary for the regulation of ICT implants. An important principle mentioned in the opinion is the precautionary principle. It also points out serious problems concerning security, privacy and data protection when using ICT implants.

Criminal law

Directive 98/84 on the protection of services based on conditional access deals with the legal protection of all those services whose remuneration relies on conditional access, such as information society services. This legal protection is important, since many services in an AmI world will rely on conditional access.

The *Cybercrime Convention of 23 November 2001* obliges the Parties to create the necessary substantive legislation and other measures to establish as criminal offences: offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences, such as computer-related forgery and computer-related fraud; offences related to child pornography; offences related to infringements of copyright and related rights; attempting and

aiding or abetting the commission of any of the above described offences; it also obliges the Parties to establish under certain conditions corporate liability for the above mentioned offences. It imposes a general obligation on the Contracting Parties to adopt legislative and other measures as may be necessary to establish the powers and procedures for the purpose of specific criminal investigations or proceedings and states that parties have to respect privacy in criminal investigations and proceedings concerning cyber crimes. The Convention finally 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. General principles are set out concerning international co-operation, extradition, mutual assistance and spontaneous information. This convention is important for AmI, since the AmI world will be one without borders and thus it is important that all countries define criminal offences in a similar way. In case of cross-border problems, the countries need to be able to co-operate with each other. While the Convention is a good initiative, its utility so far is limited by the fact that so few countries have ratified it.

Jurisdiction and applicable law

The Convention of Rome on the Law Applicable to Contractual Obligations contains rules on the applicable law in case of cross-border legal issues, but only in contractual relationships. 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 exceptions to these general rules in the case of specific contracts such as consumer contracts and individual employment contracts. An important question for our research 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. The impact of this convention is limited for AmI, since the majority of privacy and security infringements and ID thefts do not occur in contractual relationships.

Regulation 44/2001 on jurisdiction and enforcement aims to unify the rules of conflict of jurisdiction in civil and commercial matters and to simplify the formalities with a view to rapid and simple recognition and enforcement of judgments. It covers both contractual and extra-contractual matters apart from well-defined matters. Jurisdiction is generally based on the defendant's domicile. A person domiciled in a Member State may, however, be sued in another Member State in matters relating to a contract, matters relating to torts, dispute arising out of the activities of the branches, agencies or other establishment. This regulation provides legal certainty about the court competent to deal with liability as a result of privacy, identity or security violations. The regulation is not sufficiently adapted to an AmI world.

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. Furthermore, although legal instruments are useful for their deterrent value and for the (possible) prosecution of offenders, they will not stop someone who is determined to

abuse the privacy of others or to use personal information for commercial gain or criminal intent no matter what the law says.

References

Ackerman, M. S. (2004). Privacy in pervasive environments: next generation labelling protocols in Personal and Ubiquitous Computing 8, No. 6, pp. 430-439.

AIRE project: http://aire.csail.mit.edu/

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.; PentikŁinen, 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.

AMIGO: http://www.ctit.utwente.nl/research/projects/telematics/other/amigo.doc/

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.; Hbig, M.,eds. (2002). Context-Aware Collaborative Environments for Next Generation Business Networks: Scenario Document. COCONET deliverable D 2.2. Enschede: Telematica Institute.

Bardram, J. E. (2004): The Personal Medical UnitA 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.

Beckwith, R. (2003). Designing for Ubiquity: The Perception of Privacy in IEEE Pervasive Computing 2, No. 2, pp. 40-46.

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.

Cabrera Girldez, M.; Rodrguez 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.

eLearning (2003). http://europa.eu.int/comm/education/programmes/elearning/projects_descr_en.html#2003_ML

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.; 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.

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.

Gustavsson P., Lundin J., Nulden U., Taghizadeh F. (2001). Mobile Scenarios: Supporting Collaborative Learning among Mobile People. In proceedings of IRIS 24, Ulvik, Norway, vol. II, pp. 59-72

Harrop, P. (2005): Item level RFID: The business benefits of the "tag everything" scenario. Cambridge: IDTechEx Ltd.

http://www.atstake.com/research/reports/acrobat/atstake_gprs_security.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.

InterLiving project: http://interliving.kth.se

iRoom: https://graphics.stanford.edu/papers/iwork-overview/

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).

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

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.

Jernstrm, 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). Gteborg: 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/.

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, pp. 30-41.

Lashina, T. (2004): Intelligent Bathroom. In: EUSAI 2004, Workshop "Ambient Intelligence Technologies for Well-Being at Home", Eindhoven University of Technology, The Netherlands.

Lopez de Vallejo, I. (2004). E-Locus: a clustered view of European ICT for future workspaces. E-Locus Deliverable D5.5. Guipzcoa: Fundacin TEKNIKER. http://e-locus.fundaciontekniker.com/ downloads/documents/elocuspublishablereport1.pdf

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.

Marx, G. T. (2001): Murky Conceptual Waters: the Public and the Private. In: Ethics and Information Technology 3, No. 3, pp. 157-169.

Masera, M.; Bloomfeld, R.,eds. (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.

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.

MiMe project: www.mimeproject.org

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.

Mosaic: http://www.mosaic-network.org/pub/bscw.cgi/d63325/Mobility@Work%20Flyer.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.

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).

Nissenbaum, H. (2004): Privacy as Contextual Integrity. In: Washington Law Review 79, No. 1, pp. 101-139.

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.

Philips HomeLab: http://www.smarthouse.com.au/articlesbytopic/homecinema/ lcdandplasmatv/1385

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 .

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.

RUNES: www.ist-runes.org

Sachinopoulou, A.; MŁkelŁ, S.; JŁrvinen, 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 Jos, CA.

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.

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.

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.; Geiler, 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.

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.

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.

WearIT@work: http://www.wearitatwork.com/Maintainance.29.0.html

Weiser, M. Some Computer Science Issues in Ubiquitous Computing in Communications of the ACM 36, No. 7, 1993. pp. 75-85.

Whitehouse, O. (2002). GPRS Wireless Security: Not Ready for Prime Time. Research report. Boston, Denver: @Stake, Inc.

Winters, N. (2004). Personal Privacy and Popular Ubiquitous Technology in Proceedings of Ubiconf 2004, Gresham College, London. 19 April 2004.

WorkSpace: http://www.daimi.au.dk/workspace/index.htm