Privacy, Identity and Security in Ambient Intelligence: A Scenario Analysis

Michael Friedewald [a,*], Elena Vildjiounaite [b], Yves Punie [c], David Wright [d]

[a] *Fraunhofer Institute for Systems and Innovation Research, Breslauer Straße 48, 76139 Karlsruhe, Germany*

[b] *Technical Research Centre of Finland, VTT Electronics, Kaitoväylä 1, 90571 Oulu, Finland*

[c] *European Commission/DG JRC, Institute for Prospective Technological Studies, Edificio EXPO, C/Inca Garcilaso, 41092 Seville, Spain*

[d] *Trilateral Research & Consulting, 12 Tybenham Road, London, SW19 3LA, United Kingdom*

Received 19 August 2005; received in revised form 8 December 2005; accepted 16 December 2005.

Abstract

The success of Ambient Intelligence (AmI) will depend on how secure it can be made, how privacy and other rights of individuals can be protected and how individuals can come to trust the intelligent world that surrounds them and through which they move. This article addresses these issues by analysing scenarios for ambient intelligence applications that have been developed over the last few years. It elaborates the assumptions that promotors make about the likely use of the technology and possibly unwanted side effects. It concludes with a number of threats for personal privacy that become evident.

Key words: Ambient intelligence, privacy, security, scenarios, ubiquitous computing

1 Introduction

Privacy, identity, security and trust are central key issues in ambient intelligence 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 ambient intelligence stems from two innovations necessary to its success: the enhanced ability to collect data on people's everyday interactions (in multiple modalities and over large spans of time and space) and an enhanced ability to quickly search large databases of that collected data,

* Corresponding author. Tel.: +49 721 6809 146; fax: +49 721 6809 315.
Email address: m.friedewald@isi.fraunhofer.de (Michael Friedewald).

creating greater possibilities for personal profiling, and other forms of data mining (Bohn et al., 2004). One leading researcher in the field has identified a set of generic privacy concerns that ambient intelligence 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, ambient intelligence will require the tracking and collection of significant portions of users' everyday activities.

It has to be noted that many of the foreseen concerns unfold as the technology develops. As of today, they seem to be still far away and some visions sound even like science fiction. However it is important to deal with them early on in order to shape the future in a desirable way. To understand the directions of thinking of AmI and its inherent threats, a screening of more than 70 R&D projects and roadmaps, many of which have scenarios was undertaken – most of them from EU-funded research projects like the "Disappearing Computer Initiative".

In the analysed papers the AmI vision of everyday life 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, 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 analysed the AmI vision from numerous papers and which dimensions of scenarios we consider especially important. Next, we present the main application domains, their visions, and the specifics of their visions. After that, we address the main benefits, threats and open issues identified in the scenarios.

2 Aspects of privacy

From a principal point of view, privacy is generally considered to be an indispensable ingredient for democratic societies. This is because it is seen to foster the plurality of ideas and critical debate necessary in such societies. Bohn et al. (2004) refer to the work of Lessig (2000) and 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 personal information.

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".

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.

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. (2004) say 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 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.

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 an adult's life, 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. 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 further. 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.

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 may seem to be beneficial, since it reduces the amount of useless and annoying advertisements. However, this may be not so innocent or beneficial in the long term because advertisers views people as bundles of desires

to buy more, and may result in diminishing people's capacities of reasoned choice and thoughtful action.

3 Analytical framework

Producing scenarios is generally 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 at least three 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 scenarios by the IST Advisory Group et al. (2001)) or scenarios developed by projects aiming at presentation of a project goal.

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.

The third and most common types are not scenarios in the strict sense. They do not present concise storylines but rather describe situations and/or drivers or trends that may give rise to relevant AmI applications. (See, for instance, Michahelles et al. (2003) on how technology may help 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. However, it would be a mistake to miss such approaches because they show existing prototypes.

For the decomposition and analysis of visions and scenarios from numerous sources, the following dimensions were explored in the texts:

- the personality of the main *actors*, 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 small children do not 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 behavioural restrictions as in public places;
- the *activity* described in the scenario, because activity is an important part of a personal context;
- the *information flow* in the scenario, because many privacy threats are associated with disclosure of information;

- the *control level* of the envisaged AmI system, because it leads to higher dependability on AmI and because it raises a lot of questions about legal responsibility for actions taken by the technical system. This also affects humans' acceptance of AmI;
- *enabling technology* because many privacy threats are associated with the actual system implementation.

Before focussing on privacy, identity and security matters, application of AmI in domains like home, work, health, shopping, and mobility are described in general.

4 Future visions

4.1 Home application domain

Home, being the most private place for people, needs to be designed carefully because the home atmosphere is important for personal happiness and development. If a spy wants sensitive personal information about somebody, the best way to get it is to observe that person at home. Many financial and private affairs are discussed or dealt with from home, personal vulnerabilities, strengths and health problems can be seen easily, and it is difficult to say 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 (2004) said, this privacy aspect is very important for personal development.

Many AmI projects and roadmap scenarios are targeted at supporting the home environment (Friedewald et al., 2005a) in the following ways:

- providing communications between people, both between house inhabitants and between people inside and outside the house. The communications capabilities present in future homes are mainly aimed at building connections between friends, family members and relatives. This means transmitting real personal data in large quantities (Åkesson et al., 2001; IST Advisory Group et al., 2001; Ma et al., 2005; Masera and Bloomfeld, 2003);
- providing personalised access to external information of all kinds;
- helping in finding of personal belongings, e.g., toys or lost keys (Orr et al., 1999; Åkesson et al., 2001);
- controlling diverse home appliances and numerous household objects for making household duties and maintenance tasks easier (Åkesson et al., 2001; Masera and Bloomfeld, 2003);

- increasing safety and security by tracking people, appliances and objects; preventing or fast reporting of accidents; handling access control (Åkesson et al., 2001; ITEA, 2004);
- entertainment and increasing comfort levels (Åkesson et al., 2001; Palmas et al., 2001; ITEA, 2004).

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.

4.2 Work application domain

The work domain has three noteworthy aspects: first, people spend a lot of time working, but they are less free to choose in their working environment than in 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.

However the border between the private and the work sphere is not clear-cut. It is difficult to avoid doing some personal things at work because working hours are more or less the same everywhere and children may need parental permission or advice during working hours, etc. Thus, it follows that intellectual property is not the only aspect that should be considered and adequately dealt with in a working environment. Personal affairs need to be protected as well.

The analysis of research projects targeted at developing AmI at work shows that AmI-based working environments are already being implemented in some places. It can thus be expected that most people will work in a smart environment much sooner than live in a smart home. Consequently, safeguards of privacy at work are of higher short-term importance.

AmI projects and roadmap scenarios target the future work environment in the following ways (Aschmoneit and Höbig, 2002; López de Vallejo, 2004; Luff et al., 2004; Heinonen, 2004):

- 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;

- support for the 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;
- 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 available virtually everywhere in the world, employees can be reached wherever they are and they, in turn, can access their office from virtually anywhere. The office environment is generally a semi-public place, but even so, employees often perceive "their" office or cubicle as semi-private with fewer behavioural constraints than in a purely public space.

4.3 Health application domain

The health domain has two aspects: on the one hand, health care determines the life and death of people, and fast access to a person's health information (e.g., allergies and chronic diseases) can be very important in case of emergency. On the other hand, health information is highly sensitive. People may be unwilling to reveal their health problems even to close relatives, let alone to work superiors or insurance companies. Thus, it is important (but maybe not so easy) to build AmI applications in the health domain so that emergency workers and doctors can access personal information whenever needed, but nobody else can do so without authorisation (Casert, 2004).

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 (Savidis et al., 2001; ITEA, 2004; Riva, 2003; Cabrera Giráldez and Rodríguez Casal, 2005);

- cure of diseases, especially directed towards short-term recovery. Cure starts from diagnosis 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. For these cases, a continuous monitoring of vital signals is needed (Riva, 2003; Savidis et al., 2001; Jafari et al., 2004; Van Laerhoven et al., 2004);
- 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) (Morganti and Riva, 2005; Cabrera Giráldez and Rodríguez Casal, 2005; Riva, 2003);
- optimising the alarm chain in case of an emergency (e.g., heart attack or an accident), from calling for help to preparing the treatment (Savidis et al., 2001).

4.4 Shopping application domain

Ambient intelligence applications in shopping and commerce aim at creating a user-friendly, efficient and distributed service support to the customer, such as managing the search for and selection of vendors by the customer, and handling order and payment processes.

A commercial transaction covers a complex range of activities from the moment a customer enters a shop to product selection, purchase, billing, shipping and possible return of merchandise. The main AmI-enabled services provided to a customer are the following:

- personal shopping management supports the customer to compile items for purchase by intelligently surveying the stocks of food and other goods in the household and linking them intelligently with information about the customer's preferences and habits, which are collected by profiling customers (Åkesson et al., 2001; IST Advisory Group et al., 2001);
- 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 (Harrop, 2005);
- 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 (IST Advisory Group et al., 2001).

Similar to other application domains, shopping is envisioned to be possible as a remote activity from any place and any time. Scenarios that describe shopping by physically visiting shops do not specify their 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 do not mention this explicitly.

4.5 Mobility application domain

The ITEA Technology roadmap on Software Intensive Systems (ITEA, 2004) includes a vision of "nomadic applications" with 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). Mobile AmI applications have two aspects: first, people are not free to control the environment where they move.

Second, people travel both for work purposes and for their own pleasure. 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 technologies are already becoming reality today in the form of biometric passports, supported by governmental financing, which will soon become obligatory in Europe.

AmI is envisioned as supporting the following in the mobility domain (ITEA, 2004):

- 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 means to be highlighted are 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 (Luck et al., 2003);

- 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;
- 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.

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. Generally, this implies that the environment is neither public nor private, rather it can be semi-private or it can switch between public and private spheres frequently.

4.6 Leisure and entertainment application domain

Enhanced and enriched leisure and entertainment services for the consumer mass market is so far the first driver for many of the AmI technologies and could well be one of the more promising commercial markets for AmI, given its potential volume. Many of the functions AmI can provide might in the future converge into 'total' experiences whereby the traditional boundaries between culture and entertainment, or information and communication become blurred. But at the same time, this mass market might be one of the most difficult to address, particularly given the price-sensitivity of consumers.

The driving forces can still be different, however, as the leisure and entertainment sector, together with communication facilities, are more shaped by commercial interest and private industries than by cultural heritage, participation and socialisation. It is also worth noting that entertainment services rather address passive audiences than active users. But this might exactly constitute one of the challenges for AmI, as it should be in a laid-back mode (IST Advisory Group, 2002, 26).

AmI could, for instance:

- Enhance and personalise the experience of visiting historical sites, museums and exhibitions (Sparacino, 2001; Chervest et al., 2002);
- Increase access to, retrieval of and control over multimedia and cross-media content (Ardissono et al., 2004);

- Make possible self-customisation of content and context-aware entertainment, e.g. selecting music or programming that fits a person's mood by relating a songs emotional feel to quantifiable musical features such as tempo and beat intensity (Sleeth, 2002);
- Provide more immersion towards "total experiences", e.g. via 3-D real-time holographic and via cross-media content (Sleeth, 2002);
- Offer context-aware and location-based games and infotainment (Naaman et al., 2004; Adomavicius et al., 2005);

5 Results of the scenario analysis

The preceding section has shown the functions and context of AmI in different application domains. The specific privacy threats and social implications in any application domain will be analysed in the next sections.

5.1 The envisioned user population

Most of the scenarios we analysed feature ordinary working people, and it is assumed that most people, including the elderly, will 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 etc. are often described as an individual activity of a healthy, well-off adult.

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 (ITEA, 2004, pp. 134ff.). 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 (Savidis et al., 2001). 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 (Åkesson et al., 2001). The roles of children in the 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. This neglects the important role that youngsters have always played in the adoption of new media (e.g. SMS).

Health care scenarios 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 pattern is that a person's problems or disabilities are described as if there was only 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 and can afford the new technologies.

5.2 Level of personal control over technology

The level of control that a person has over the AmI system may vary considerably depending of the application. 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 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 do not present explicit user interactions with AmI systems where the user is granted access rights and control over personal data, thus, it is assumed that AmI has high level control over privacy issues).

Applications where a person's life depends on AmI and where AmI has a high level of control include safe mobility, especially driving (AmI detects obstacles, controls car speed and ensures that the car stays on the road), health monitoring and detection of a health crisis (such as heart attack). Generally, in driving scenarios, it is not clear if users are free to organise their travel means, time and route. Scenarios

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

An important feature of AmI with high-level control is personalisation, which can be applied for adjusting an environment (lighting, heating); for filtering of shopping advertisements and selection of TV programs. An important question about personalisation is, however, not the degree of AmI vs. personal control, but the question about who is in control of the AmI system. Whether in shopping, or in news filtering, or in recommendations about medicines, trips, etc., how are the user's interests protected and how is it ensured that information is objective? At the moment, privacy protection activists have severe doubts about the customer's control of AmI-enabled shopping services (Albrecht and McIntyre, 2005). 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 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 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 situations, and whether people will rely too much on simulators instead of using their own imagination and creativity.

5.3 Information flow

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, protection of professional secrets, or access to health data) and which mention biometric sensors do not 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 during the authentication process. The presence of identity information in multiple locations increases a risk of identity theft, particularly when one takes into account the fact that currently information stored in personal devices is poorly protected.

Another very popular element of scenarios is the presence of information about a person's or object's location and/or destination. Most often, it is processed locally, in the user device or in the car, but it can also be transmitted to a service provider. Tracking of workers' location and location of work-related objects 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 the automatic payment of road tolls and other 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 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 physi-

cian's surgery and in the hospital. During this ad hoc communication, the most sensitive information (identity, health history, etc.) is exchanged. Second, mobile emergency systems use ad hoc communication with third party nodes as relays for data transmission (e.g. in 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 (e.g. in Palmas et al., 2001), and in such cases, the data might not be protected at all.

Less sensitive data, but also of high interest and economic value to diverse organisations and different people, are collected for personalisation purposes, stored either on a personal device or in a central database (e.g., customers' data are often stored in a retailer's database) and often exchanged for providing personalised services. This information includes user profiles created from the collected data about shopping behaviour; travel preferences; user profiles created from web surfing, watching TV; and from e-learning exercises. Such data can reveal a lot about a person's psychology, lifestyle, finances, health and intelligence, especially when matched with information from other sources.

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. Such data is less sensitive than a person's identity data. However, they are of high interest to many more people and organisations because the data has 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 Threats in a World of Ambient Intelligence

Almost all analysed scenarios postulate or assume benefits of ambient intelligence while only a minority refers explicitly to the threats associated with AmI at the same time. In almost all cases, it is mentioned between the lines that also threats exist, bacause it is always assumed that 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 inevitably increasing in the AmI world and, consequently, privacy protection should be built into AmI systems rather than relying only on user control over personal data. While one should assume a certain awareness of users about information flows and 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-dependent, 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.

Apart from the following indicative list of threats Ambient Intelligence is raising numerous legal issue in the fields of data protection, torts and liability, intellectual property rights, consumer protection etc. (for more detailed analysis see Friedewald et al., 2005b, Chap. 4).

6.1 Surveillance of users

The availability of data about virtually every citizen can provoke the desire of governments to access the data for the administering their welfare systems, in law enforcement and the fight against terrorism. Other institutions like health insurances may justify their actions on similar grounds (even when their actions are at least questionable). Since AmI applications are envisaged to be implemented in many spheres of life – even those where privacy has been considered sacrosanct such as

in the home – it should come as no surprise that some critics raise the spectre of an Orwellian police state.

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

The possibility of a retailer being able to monitor the shopping behaviour of customers can not only lead to an optimised supply chain, it may also be the basis of the "transparent customer" who can be manipulated and controlled. Critics fear that the providers who are in control of the AmI infrastructure use it only for their own benefit by leading their customers to products they want to promote rather than to the products that the customers need or could benefit from (Albrecht and McIntyre, 2005). Market transparency due to more information as envisioned by most proponents of the AmI world of shopping may be foiled by the effects on the supply side like favourable purchase conditions only for selected groups while others might be disadvantaged or even excluded from the benefits of AmI-enabled shopping.

Some of the scenarios argue that it is useful for the user to know if an acquaintance is in the vicinity. Maybe so, but the downside is that disclosure of a person's position can not only threaten his/her 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).

6.2 Identity theft

Identity theft is the act of obtaining identity information without the concerned person's consent and for future activities criminal or not (intent). The more widely personal information becomes available, the greater is the risk of it 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 more

severe, 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 their data for any kind of fraud, for terrorist attacks and even harm the life and health of the victims.

Even worse, 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.

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 a stolen wallet or purse or information in your home or car, theft is obvious but in other cases the discovery comes later, by monitoring bank accounts, by company notification, by a refusal for a loan application, etc.

6.3 Malicious attacks

The term “malicious attack” subsumes a number of ways in which people attempt to access or damage a computer, mobile phone or other device. Such attacks can take many forms, can be active or passive. An active attack is a deliberate alteration or destruction of data or creation of false data. A passive attack consists of unauthorized monitoring, but not alteration or destruction of data (e.g., wiretapping).

Especially complex systems like the ones described in many scenarios can become a target of active attacks (viruses, denial of service), resulting in a failure of parts or the complete AmI system. This may lead to 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 the consequences;

- 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 for some time.

Thus, as 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.

6.4 Digital divide

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

People may be forced to use AmI technology. The pressure to use AmI may be direct as in the case in which for example, (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 loneliness, especially of 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.

The deployment of AmI also challenges the relationship between different group and/or family members. 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?

Finally, 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 can offer – even in fields that have been regarded as having public utility. This is especially relevant in the field of education where society could be divided more sharply into well-educated and less well-educated people.

7 Conclusions

The main conclusion from our analysis is that ambient intelligence technology goes beyond most of currently existing privacy-protecting borders.

First, increased connectivity between people and spaces blurs physical borders of observability such as walls and doors. A well-known example for this development are experiments in computer-supported collaborative work, namely, installation of video cameras in offices with the goal to increase awareness between colleagues and make communications between them more natural and more frequent. These experiments have shown that people forget easily about always-on video cameras, especially because the intuitive expectation "If I can not see you, then you can not see me" does not apply to computer-mediated communications (Bellotti and Sellen, 1993), and this threatens personal privacy.

Second, the physiological sensors, always on, always attached to a person (whether for the goal of health monitoring or for personalising TV and learning programs), make this person absolutely helpless to hide his/her feelings because feelings can be discovered from changes in physiological parameters (Nasoz et al., 2003). This means that facial expressions do not constitute a natural border protecting true personal feelings anymore.

Third, the blurring of boundaries between time and space, recording and storing many kinds of information in AmI systems and increased capacity of data mining algorithms (which enable the finding of relationships and connections between diverse and seemingly unrelated pieces of data) violate personal expectations about spatial and temporal privacy-protecting borders, as well as expectations concerning ephemerality and transience of events.

New technologies will inevitably change personal expectations concerning privacy generally. Nissenbaum (2004) cites a U.S. court decision as an example of such changes. The court decided that the police did not violate personal private space when they discovered an illegal activity while flying an airplane over a person's home and yard, because one cannot expect reasonable privacy from surveillance planes since flights have become a common part of our lives. So, what kind of changes in privacy expectations will replace the current expectations when AmI technologies become a common part of our lives? Whatever they will be, changes in

people's expectations of privacy will happen more slowly than technology capabilities grow, as experiments in computer-supported collaborative work have shown.

Acknowledgement

This work is supported by the EU project SWAMI: Safeguards in a World of Ambient Intelligence (IST-2004-006507). Important contributions to this work came from Ioannis Maghiros and Sabine Delaitre (EC/DG JRC, IPTS), Petteri Alahuhta (VTT Electronics) and Ralf Lindner (Fraunhofer ISI). The views expressed are purely those of the writers and may not in any circumstances be regarded as stating an official position of the European Commission.

References

Åkesson, K.-P., Humble, J., Crabtree, A., Bullock, A., 2001. Usage and development scenarios for the tangible toolbox. ACCORD Deliverable D1.3, Swedish Institute of Computer Science.

Ackerman, M. S., 2004. Privacy in pervasive environments: Next generation labelling protocols. Personal and Ubiquitous Computing 8 (6), 430–439.

Adomavicius, G., Sankaranarayanan, R., Sen, S., Tuzhilin, A., 2005. Incorporating contextual information in recommender systems using a multidimensional approach. ACM Transactions on Information Systems 23 (1), 103–145.

Albrecht, K., McIntyre, L., 2005. Spychips: How Major Corporations and Governments Plan to Track Every Move with RFID. Nelson Current, Nashville.

Ardissono, L., Gena, C., Torasso, P., Bellifemine, F., Chiarotto, A., Difino, A., Negro, B., 2004. User modeling and recommendation techniques for personalized electronic program guides. In: Ardissono, L., Kobsa, A., Maybury, M. T. (Eds.), Personalized Digital Television: Targeting programs to individual users. Kluwer, Dordrecht, London.

Aschmoneit, P., Höbig, M., September 26 2002. Context-aware collaborative environments for next generation business networks: Scenario document. COCONET Deliverable D 2.2, Telematica Institute.

Beckwith, R., 2003. Designing for ubiquity: The perception of privacy. IEEE Pervasive Computing 2 (2), 40–46.

Bellotti, V., Sellen, A., 1993. Design for privacy in ubiquitous computing environments. In: Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93). Kluwer, pp. 77–92.

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., Rohs, M., 2004. Living in a world of smart everyday objects: Social, economic, and ethical implications. Journal of Human and Ecological Risk Assessment 10 (5), 763–786.

Cabrera Giráldez, M., Rodríguez Casal, C., 2005. The role of ambient intelligence in the social integration of the elderly. In: Riva et al. (2005), pp. 265–280.

Casert, R., December 2004. Workshop ambient intelligence: In the service of man? Societal aspects of ambient intelligence in the field of health and surveillance. Rep. RP-DIV-167, Rathenau Institute, The Hague.

Chervest, K., Davies, N., Mitchell, K., 2002. The role of adaptive hypermedia within a context-aware tourist guide. Communications of the ACM 45 (5), 47–51.

Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P., Heinonen, S., 2005a. Perspectives of ambient intelligence in the home environment. Telematics and Informatics 22 (3), 221–238.

Friedewald, M., Vildjiounaite, E., Wright, D., Maghiros, I., Verlinden, M., Alahuhta, P., Delaitre, S., Gutwirth, S., Schreurs, W., Punie, Y., July 2005b. Safeguards in a world of ambient intelligence (SWAMI): The brave new world of ambient intelligence – A state-of-the-art review. Deliverable D1, Fraunhofer ISI. http://swami.jrc.es

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

Heinonen, S., 2004. Mobile telework at the crossroads of social, environmental and cultural challenges. In: 9th International Telework Workshop, International Telework Academy, Crete, Greece, 6th - 9th September, 2004.

IST Advisory Group, June 2002. Strategic orientations and priorities for IST in FP6. Office for Official Publications of the European Communities, Luxembourg.

IST Advisory Group, Ducatel, K., Bogdanovicz, M., Scapolo, F., Leijten, J., Burgelman, J.-C., February 2001. Scenarios for ambient intelligence in 2010. Institute for Prospective Technological Studies (IPTS), Seville.

ITEA, May 2004. ITEA technology roadmap for software-intensive systems, 2nd edition. Information Technology for European Advancement (ITEA) Office Association, http://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, Nottingham, 7 September 2004.

Lessig, L., 2000. Code and other laws of cyberspace. Basic Books, New York.

López de Vallejo, I. L., September 2004. E-locus: A clustered view of European ICT for future workspaces. E-Locus Deliverable D5.5, Fundación TEKNIKER.

Luck, M., McBurney, P., Preist, C., January 2003. Agent Technology: Enabling Next Generation Computing. A Roadmap for Agent Based Computing. AgentLink, Southampton.

Luff, P., Heath, C., Norrie, M., Signer, B., Herdman, P., 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 2004. pp. 523–532.

Ma, J., Yang, L. T., Apduhan, B. O., Huang, R., Barolli, L., Takizawa, M., 2005. Towards a smart world and ubiquitous intelligence: A walkthrough from smart things to smart hyperspaces and ubickids. International Journal of Pervasive Computing and Communications 1 (1).

Masera, M., Bloomfeld, R., August 2003. A dependability roadmap for the Information Society in Europe. AMSD Delilverable D1.1, Rand Europe.

Michahelles, F., Matter, P., Schmidt, A., Schiele, B., 2003. Applying wearable sensors to avalanche rescue: First experiences with a novel avalanche beacon. Computers & Graphics 27 (6), 839–847.

Morganti, F., Riva, G., 2005. Ambient intelligence for rehabilitation. In: Riva et al. (2005), pp. 281–292.

Naaman, M., Harada, S., Wang, Q., Garcia-Molina, H., Paepcke, A., 2004. Context data in geo-referenced digital photo collections. In: Proceedings of the 12th annual ACM international conference on Multimedia, New York, NY, USA. pp. 196–203.

Nasoz, F., Alvarez, K., Lisetti, C., Finkelstein, N., 2003. Emotion recognition from physiological signals for user modelling of affect. In: Proceedings of the 3rd Workshop on Affective and Attitude User Modelling (Pittsburgh, PA, USA, June 2003).

Nissenbaum, H., 2004. Privacy as contextual integrity. Washington Law Review 79 (1), 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 Center, Georgia Tech.

Palmas, G., Tsapatsoulis, N., Apolloni, B., Malchiodi, D., Delopoulos, A., Beverina, F., 30 September 2001. Generic artefacts specification and acceptance criteria. Oresteia Deliverable D01, STMicroelectronics s.r.l.

Riva, G., 2003. Ambient intelligence in health care. CyberPsychology and Behavior 6 (3), 295–300.

Riva, G., Vatalaro, F., Davide, F., Alcaiz, M. (Eds.), 2005. Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction. Vol. 6 of Studies in New Technologies and Practices in Communication. IOS Press, Amsterdam.

Savidis, A., Lalis, S., Karypidis, A., Georgalis, Y., Pachoulakis, Y., Gutknecht, J., Egger, B., Kramer, P., Tafra, M., Majoe, D., Lieu, V., Hunt, N., Gredmaier, L., Roberts, D., 2001. Report on key reference scenarios. 2WEAR Deliverable D1, Foundation for Research and Technology Hellas, Institute of Computer Science.

Singer, I. J., 2001. Privacy and human nature. Ends and Means 5 (1).

Sleeth, C. E., 2002. Technology map: Pervasive computing. SRI Consulting Business Intelligence, Menlo Park, Croydon, Tokyo.

Sparacino, F., 2001. Sto(ry)chastics: a bayesian network architecture for combined user modeling, sensor fusion, and computational storytelling for interactive spaces. Ph.D. thesis, Massachussetts Institute of Technology.

Van Laerhoven, K., Lo, B. P. L., Ng, J. W. P., Thiemjarus, S., King, R., Kwan, S., Gellersen, H., Sloman, M., Wells, O., Needham, P., Peters, N., Darzi, A., Toumazou, C., Yang, G.-Z., 2004. Medical healthcare monitoring with wearable and implantable sensors. In: UbiHealth 2004 - The 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Nottingham, 7 September 2004.

Weiser, M., 1993. Some computer science issues in ubiquitous computing. Communications of the ACM 36 (7), 75–85.

Winters, N., 2004. Personal privacy and popular ubiquitous technology. In: Proceedings of Ubiconf 2004, April 19th, Gresham College, London.