The Brave New World of Ambient Intelligence: An Analysis of Scenarios Regarding Privacy, Identity and Security Issues

Michael Friedewald[1], Elena Vildjiounaite[2], Yves Punie[3], and David Wright[4]

[1] Fraunhofer Institute for Systems and Innovation Research,
Breslauer Straße 48, 76139 Karlsruhe, Germany
[2] Technical Research Centre of Finland, VTT Electronics,
Kaitoväylä 1, 90571 Oulu, Finland
[3] European Commission/DG JRC, Institute for Prospective Technological Studies,
Edificio EXPO, C/Inca Garcilaso, 41092 Seville, Spain
[4] Trilateral Research & Consulting, 12 Tybenham Road,
SW19 3LA, United Kingdom, London

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 contribution presents an analysis of ambient intelligence scenarios, particularly in regard to AmI's impacts on and implications for individual privacy. The analysis draws on our review of more than 70 AmI projects, principally in Europe. It notes the visions as well as the specifics of typical AmI scenarios. Several conclusions can be drawn from the analysis, not least of which is that most AmI scenarios depict a rather too sunny view of our technological future. Finally, reference is made to the SWAMI project (Safeguards in a World of Ambient Intelligence) which, inter alia, has constructed "dark" scenarios, as we term them, to show how things can go wrong in AmI and where safeguards are needed.

1 Introduction

The term Ambient Intelligence (AmI) was coined by Emile Aarts of Philips and taken up by the Advisory Group to the European Community's Information Society Technology Program (ISTAG) as the convergence of ubiquitous computing, ubiquitous communication, and interfaces adapting to the user. The concept of AmI depicts a vision of the future information society, where the emphasis is on greater user-friendliness, more efficient services support, user empowerment, and support for human interactions. People are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects and an environment that is capable of recognising and responding to the presence of different individuals in a seamless, unobtrusive, and often invisible way [1, 2].

Privacy, identity, security and trust are central key issues in ambient intelligence visions and have been identified as such from their earliest inception [3].

J.A. Clark et al. (Eds.): SPC 2006, LNCS 3934, pp. 119–133, 2006.

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, creating greater possibilities for personal profiling, and other forms of data mining [4]. One leading researcher in the field has identified a set of generic privacy concerns that ambient intelligence will very likely raise for users [5]:

- 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 developed scenarios, was undertaken – most of them from EU-funded research projects such as the "Disappearing Computer Initiative" [6, 7, 8, 1, 9, 10, 11, 12, 13, 14, 15, to name the most important].

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.

Before detailing our analytic approach to deconstructing AmI scenarios, we present in the following section the views of several researchers on privacy and its aspects.

2 Aspects of Privacy

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. [4] refer to the work of Lessig [16] 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. [4] 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 [17] 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 [18] 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 view people as bundles of desires to buy more, and may result in diminishing people's capacities of reasoned choice and thoughtful action.

3 Deconstructing AmI Scenarios

3.1 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 ISTAG scenarios [1]) 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 [19] 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 [20]:

- 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.

3.2 The Envisioned AmI User Population

As there are different target groups in the scenarios, actors in the scenarios are described by their age group, health group, profession, social status and attitude towards technology. This dimension is important because social, legal and privacy issues depend on scenario actors, e.g., people with severe disabilities may be willing to exchange some privacy to get more support, and small children don't care much about privacy. On the other hand, politicians usually care much more about personal data than average people.

Most of the analysed scenarios 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 [9, pp. 134ff.]. In scenarios describing how a user is woken 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 [15]. 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 [6]. 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.

3.3 Activities and Environments in Ambient Intelligence

The typical scenarios that have been developed over the last years envision application of ambient intelligence for work, learning, ordinary everyday activities like household-related activities, changing places, leisure and hobby, social, health maintenance, emergency. This dimension is important because information flow is closely linked to the activity, and main privacy threats are related to information flow.

Home, being the most private place for people, needs to be designed carefully because the home atmosphere is important for personal happiness and development [21]. If a spy wants sensitive personal information about somebody, the best way to get it is to observe that person at home. Many financial and private affairs are discussed or dealt with from home, personal vulnerabilities, strengths and health problems can be seen easily, and it is difficult to say what information about someone can not be found in the home environment. Second, people perceive their homes as a place where they can be free from intrusion, relax and think in peace, i.e., "to be left alone". As Nissenbaum said, this privacy aspect is very important for personal development [17].

The *work* domain has three noteworthy aspects: first, people spend a lot of time working, but they are less free to choose their working environment than their home environment. If organisations choose to violate personal privacy in some way, workers can either accept it or try to find a better employer. In any case, if workers feel their privacy is violated, they can feel humiliated and depressed, and it is an open question how much an organisation will benefit or lose from close surveillance of its employees. Second, people can not avoid dealing with some personal matters during working hours, e.g., making appointments to see a doctor or a teacher of their children; talking to a mechanic about repairs to their cars; communicating with family members; reserving a table at a restaurant and so on. It is difficult to avoid doing some personal things because working hours are more or less the same everywhere and children may need parental permission or advice during working hours. Thus, it follows that intellectual property is not the only thing that should be protected in a working environment. Personal affairs also need to be protected. Third, our analysis of research projects targeted at developing AmI at work has shown that visions of the future working environment are already being implemented in some companies, hospitals and research institutes capable of investing more money than ordinary people in their homes. Thus, we can expect to work in a smart environment sooner than to live in a smart home. Consequently, safeguards of privacy at work should be developed as soon as possible.

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.

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.

In the applications of AmI for *travel and mobility* (called the "nomadic domain" by one influential scenario [9]) will have the same facilities and services as those in the home and at work, but while people are at different places temporarily or on the move (e.g., on the road). The mobility domain has two aspects: first, people are not free to control the environment where they move - governments require passports, visas, driving licences, etc; transportation companies have rules too, e.g., where to put the luggage and what can or can not be transported. AmI technologies are already becoming present in the mobility domain in the form of biometric passports, supported by governmental financing, which will soon become obligatory in Europe. Second, people travel both for work and for their own pleasure. Travel is an important feature of life today. This means that privacy protection in the mobility domain needs to be developed urgently, otherwise travellers will be left with the choice either of accepting threats to their privacy or ceasing to travel (and for those who travel for work ceasing travel is simply impossible).

All these activities do not necessarily take place in one environment, in fact it is part of the AmI vision that activities can take place at virtually any place. The environments found in the scenarios include: urban, long-distance travelling, countryside and nature. This dimension is important because in different environments different technologies are needed, and because it shows where changes can appear earlier. The dimension is also important because people have different expectations about privacy in different environments, e.g. in their own home and in the nature people are less willing to accept same behaviour restrictions as in public places.

3.4 Information Flow in AmI Applications

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 [22].

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 physician's surgery and in the hospital. During this ad hoc communication, the most sensitive information (identity, health history, etc.) is exchanged. Second, mobile emergency systems use ad hoc communication with third party nodes as relays for data transmission [15]; 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 [13], 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 become 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.

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, because 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 [23].

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.

3.5 Personal Control over AmI 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 [24]. 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.[1]

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.

A foretaste of the high level of control in the communications domain is provided in the recent EU-level decision to require telecom operators to customer data for up to 10 years. Interestingly, civil liberties groups who opposed the measure were joined by the telecom operators themselves, not because of the potential for violation of civil liberties, but on cost grounds. The operators opposed the measure because they would bear the brunt of the cost of storing such data, which according to some estimates could increase ten-fold.

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 [1], 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.

[1] The consumer protest about Sony's installing spyware on its CDs unbeknownst to consumers until Sony was exposed provides an indicative example. When it was discovered, Sony claimed that the spyware was to prevent illegal copying of music. However, the protest was such that Sony said it would withdraw the offending CDs. However, some reports say that Sony was continuing (at least as at the end of 2005) to sell such CDs [25].

The issue framed by the question: "Who is in control?" must also take into account situations where AmI technology may be used for surveillance. Instances of where the government and industry have engaged in surreptitious surveillance have come to light, e.g., Intel's encoding a unique serial number into every Pentium III microprocessor and the hidden files used to identify the authors of Microsoft Word documents [26]. One can distinguish two types of surveillance. The first type of surveillance is targeted. Targeted surveillance includes those situations where security agencies target suspected criminals or terrorists as well as surveillance cameras in the streets or shops. The second type of surveillance is not targeted. The latter type employs technologies that can be used, if needed, to identify someone. The existence or at least application of such technologies is not transparent to consumer (which distinguishes them from the surveillance cameras used to monitor motorists exceeding speed limits or used to apprehend shoplifters). The Intel numbering and Microsoft files and most spyware fall into the second category of surveillance. Of course, the surveillance may also be legal or illegal. Speed cameras are legal. Spying on citizens without a warrant is usually illegal, but even government agencies may engage in illegal activity.[2] Based on experience and history, one can only assume that some AmI technologies will also be used in a non-transparent and/or illegal way for the nefarious purposes of government and industry even when such surveillance is not warranted. Thus, even in situations where consumers think they are in control, they may not be.

4 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 [28], 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 [29]. This means that facial expressions do not constitute a natural border protecting true personal feelings anymore.

[2] Recently, the Associated Press reported that "The [US] National Security Agency's Internet site has been placing files on visitors' computers that can track their Web surfing activity despite strict federal rules banning most files of that type" [27].

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 [17] 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.

The bottom line from our analysis of existing AmI scenarios is that they have tended to paint a rather too sunny view of the future. As an antidote, the SWAMI consortium has constructed several so-called "dark" scenarios, as we call them, which highlight things that can go wrong in the deployment and application of AmI technology [30]. From our analysis of existing scenarios as well as of our own dark scenarios, we conclude that a range of safeguards are needed to better protect privacy and re-assert greater user control [31]. Identifying and elaborating needed safeguards are the focus of our research in 2006.

Acknowledgement

This work is supported by 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

[1] IST Advisory Group, Ducatel, K., Bogdanovicz, M., Scapolo, F., Leijten, J., Burgelman, J.C.: Scenarios for ambient intelligence in 2010. Institute for Prospective Technological Studies (IPTS), Seville (2001). http://www.cordis.lu/ist/istag-reports.htm

[2] Punie, Y.: The future of ambient intelligence in Europe: The need for more everyday life. Communications and Strategies **57** (2005) 141–165

[3] Weiser, M.: Some computer science issues in ubiquitous computing. Communications of the ACM **36** (1993) 75–85

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

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

[6] Åkesson, K.P., Humble, J., Crabtree, A., Bullock, A.: Usage and development scenarios for the tangible toolbox. ACCORD Deliverable D1.3, Swedish Institute of Computer Science (2001). http://www.sics.se/accord/plan/del/D1.3.pdf

[7] Aschmoneit, P., Höbig, M.: Context-aware collaborative environments for next generation business networks: Scenario document. COCONET Deliverable D 2.2, Telematica Institute (2002). http://coconet.telin.nl/

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

[9] ITEA: ITEA technology roadmap for software-intensive systems, 2nd edition. Information Technology for European Advancement (ITEA) Office Association (2004). http://www.itea-office.org

[10] López de Vallejo, I.L.: E-locus: A clustered view of European ICT for future workspaces. E-Locus Deliverable D5.5, Fundación TEKNIKER (2004). http://e-locus. fundaciontekniker.com/

[11] Masera, M., Bloomfeld, R.: A dependability roadmap for the Information Society in Europe. AMSD Delilverable D1.1, Rand Europe (2003). https://rami.jrc.it/roadmaps/amsd/

[12] Morganti, F., Riva, G.: Ambient intelligence for rehabilitation. In Riva, G., Vatalaro, F., Davide, F., Alcaiz, M., eds.: Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction. IOS Press, Amsterdam (2005) 281–292

[13] Palmas, G., Tsapatsoulis, N., Apolloni, B., Malchiodi, D., Delopoulos, A., Beverina, F.: Generic artefacts specification and acceptance criteria. Oresteia Deliverable D01, STMicroelectronics s.r.l. (2001). http://www.image.ece.ntua.gr/ oresteia/

[14] Riva, G.: Ambient intelligence in health care. CyberPsychology and Behavior **6** (2003) 295–300

[15] 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.: Report on key reference scenarios. 2WEAR Deliverable D1, Foundation for Research and Technology Hellas, Institute of Computer Science (2001). http://2wear.ics.forth.gr/

[16] Lessig, L.: Code and other laws of cyberspace. Basic Books, New York (2000)

[17] Nissenbaum, H.: Privacy as contextual integrity. Washington Law Review **79** (2004) 101–139

[18] Singer, I.J.: Privacy and human nature. Ends and Means **5** (2001) 1

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

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

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

[22] Elbirt, A.J.: Who are you? How to protect against identity theft. IEEE Technology and Society Magazine **24** (2005) 5–8

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

[24] Albrecht, K.: Supermarket cards: The tip of the retail surveillance iceberg. Denver University Law Review **79** (2002) 534–539, 558–565

[25] Farrell, N.: Sony gives rootkits for christmas. The Inquirer (26 December 2005). http://www.theinquirer.net/?article=28548

[26] Borrus, A.: The privacy war of Richard Smith. Businessweek Online (14 February 2000). http://www.businessweek.com/2000/00_07/b3668067.htm?scriptFramed

[27] Associated Press: Spy agency removes illegal tracking files. The New York Times (29 December 2005). http://www.nytimes.com/2005/12/29/national/29cookies.html

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

[29] Nasoz, F., Alvarez, K., Lisetti, C., Finkelstein, N.: 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). (2003)

[30] Punie, Y., Delaitre, S., Maghiros, I., Wright, D., Friedewald, M., Alahuhta, P., Gutwirth, S., de Hert, P., Lindner, R., Moscibroda, A., Schreurs, W., Verlinden, M., Vildjiounaite, E.: Safeguards in a world of ambient intelligence (SWAMI): Dark scenarios on ambient intelligence - Higlighting risks and vulnerabilities. SWAMI Deliverable 2 (2005). http://swami.jrc.es

[31] Wright, D.: The dark side of ambient intelligence. Info - The journal of policy, regulation and strategy for telecommunications **7** (2005) 6 33–51