Safeguards in a World of Ambient Intelligence (SWAMI)

Deliverable D5

Report on the Final Conference, Brussels, 21-22 March 2006

April 2006

Editors: Michael Friedewald & David Wright

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

Partners:

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

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

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

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

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

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

Legal notice

We suggest the following citation format: Friedewald, M. & Wright, D. (eds.) "Report on the Final Conference, Brussels, 21-22 March 2006". SWAMI Deliverable D5. A report of the SWAMI consortium to the European Commission under contract 006507, April 2006. http://swami.jrc.es

Contents

Preface

David Wright[1] and Michael Friedewald[2]

[1] Trilateral Research & Consulting, 12 Tybenham Road, SW 19 3LA London, United Kingdom, david.wright@trilateralresearch.com
[2] Fraunhofer Institute Systems and Innovation Research, Breslauer Straße 48, 76139 Karlsruhe, Germany, Michael.Friedewald@isi.fraunhofer.de

This report provides the results of the Final Conference of the SWAMI project. Convened 21-22 March 2006, the conference brought together, not only the SWAMI partners, but also representatives of other AmI-related projects, officials from the European Commission, policy-makers, researchers, regulators and other opinion leaders.

The SWAMI partners were committed to the success of the Conference, because it provided an opportunity to set out, at least in summary form, the key findings of the SWAMI project and, in particular, the threats and vulnerabilities in relation to privacy, identity, trust, security and digital divide issues in the context of a World of Ambient Intelligence. We wanted to obtain the feedback and views of other AmI experts and policy-makers. We wanted to create a forum where representatives from the AmI community could exchange views about how we can ensure the success of AmI in Europe while ensuring equal opportunities and rights of all citizens and user control in the brave new world of AmI.

All SWAMI partners collaborated in putting the Conference together and participating in the proceedings. We held the Conference in Brussels in order to maximise the possibility for participation by Commission officials. In fact, the Conference was even more successful than we had hoped - we had made provision for 60 people to attend but had many more requests than that. While the Conference was attended predominantly by experts from Europe, we had participants from as far away as California and Japan. We were pleased by the informal feedback we obtained from participants, not only about the Conference itself but also about the SWAMI reports and the work which has been accomplished in the project so far. It has also been gratifying to see the interaction and collaboration which has arisen between SWAMI and other EC-supported AmI projects.

Finally, we would like to thank all participants for making the Conference a success and for their active participation in the proceedings. We hope that participants will continue to take an interest in the SWAMI project and, especially, our final report. For those who were unable to attend the Conference, we trust this report provides an adequate summary of what transpired.

Part I

The SWAMI project

Introduction to the SWAMI Project

Michael Friedewald

Fraunhofer Institute Systems and Innovation Research, Breslauer Straße 48, 76139 Karlsruhe, Germany, Michael.Friedewald@isi.fraunhofer.de

Ambient Intelligence (AmI) describes a vision of the future Information Society as the convergence of ubiquitous computing, ubiquitous communication and interfaces adapting to the user. In this vision, 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 [2].

While most stakeholders paint the promise of AmI in sunny colours, there is a dark side to AmI as well. In a way, this dark side is inherent in many technologies including AmI, where intelligence is embedded in the environment and accessible anywhere and at any time including by those on the move. In this future, virtually every product and service will be embedded with intelligence. With networking microchips tinier than a pinhead, personalised services can be provided on a scale dwarfing anything hitherto available. Taken together, these developments will create a profoundly different information landscape from the one with which we are familiar today and that will have to cope with the following key characteristics [4]:

- Complexity – as hardware capabilities improve and costs reduce, there is continuing pressure to attempt to build systems of ever greater scope and functional sophistication;
- Boundary-less nature of the systems and interconnectedness – few systems have a clear-cut boundary. They are subdivided into systems within systems;
- Unpredictability – all nodes, connected through a common infrastructure are potentially accessible from anywhere at any time, which may result in unpredictable emergent behaviours;
- Heterogeneity and blurring of the human/device boundary as, for example, wearable and/or implantable devices become more widely available and drop in cost;
- Incremental development and deployment – systems are never finished, new features (and sources of system faults and vulnerabilities) are being added at a continuous pace;

- Self-configuration and adaptation – systems are expected to be able to respond to the changing circumstances of the ambient where they are embedded.

The scale, complexity and ever-expanding scope of human activity within this new ecosystem present enormous technical challenges for privacy, identity and security – mainly because of the enormous amount of behavioural, personal and even biological data being recorded and disseminated. Moreover, many more activities in daily life, at work and in other environments, will depend on the availability of AmI devices and services. Questions of ownership and governance of infrastructures and services will thus loom large. The growing autonomy and intelligence of devices and applications will have implications for product liability, security and service definition. There will also be new and massive economic activity in the trading of those techniques that make things smart. One can expect vigorous discussions of who has rights over what information and for what purpose. Finally, there will be a constant struggle to defend this world of ambient intelligence against attacks from viruses, spam, fraud, masquerade, cyber terrorism and so forth [5]. These issues lie at heart of the SWAMI project.

SWAMI has three major tasks:

1. To identify the social, legal, organisational and ethical implications related to issues such as privacy, anonymity, manipulation and control, and identity in the context of ambient intelligence using current and future information and communications technologies [1].
2. To create and analyse four "dark" scenarios about AmI that highlight and detail the key socio-economic, legal, technological and ethical risks related to, in particular, identity, privacy and security. The scenarios are called dark because they present visions of the future that we do *not* want to become reality. Their objective is to expose risks and vulnerabilities as a way to inform policy-makers and planners about the dangers posed by these possibilities [3].
3. To identify research and policy options on how to build into Information Society services and systems the safeguards and privacy-enhancing mechanisms needed to ensure user control, user acceptance and enforceability of policy in an accessible manner, with a view to support accessibility and the provision of citizens with real equal rights and opportunities in a world of ambient intelligence.

References

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

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

[3] 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., and Vildjiounaite, E. (2005). Safeguards in a world of ambient intelligence (SWAMI): Dark scenarios on ambient intelligence – Higlighting risks and vulnerabilities. SWAMI Deliverable 2. http://swami.jrc.es

[4] Riguidel, M. and Martinelli, F. (2006). Beyond the horizon - thematic group 3: Security, dependability and trust. Report for public consultation. http://www.beyond-the-horizon.net.

[5] Sharpe, B., Zaba, S., and Ince, M. (2004). Foresight cyber trust and crime prevention project. technology forward look: User guide. Technical report, Office of Science & Technology.

Threats, vulnerabilities & safeguards in a World of Ambient Intelligence

David Wright

Trilateral Research & Consulting, 12 Tybenham Road, SW 19 3LA London, United Kingdom, david.wright@trilateralresearch.com

The third SWAMI report addresses the key issues of privacy, identity, security, trust and digital divide in an AmI world and, in particular, identifies various threats and vulnerabilities and safeguards to minimise their impacts.

The report responds to the third SWAMI objective, which is to identify research and policy options regarding safeguards and privacy-enhancing mechanisms needed to ensure user control, acceptance and enforceability of policy with equal rights and opportunities for citizens.

The presentation made by David Wright at the SWAMI conference drew on a summary paper circulated to conference participants. That paper (which is included in this conference report) highlights *privacy* threats and vulnerabilities, including the following:

- hackers & malware
- function creep
- security & surveillance
- profiling
- sharing of data between companies & government
- lack of public awareness about privacy rights
- lack of enforcement & oversight
- erosion of rights & values
- uncertainties about what to protect & costs
- uncertainties about the economic costs of privacy erosion
- lax security
- government and industry being less than forthright.

Among *identity* threats and vulnerabilities signalled by SWAMI are these:

- identity theft
- function creep
- exploitation of linkages by industry & government
- penetration of identity management systems (hacking, spoofing, denial of service, etc)

- authentication measures that intrude upon privacy
- complexity of identity management systems
- failures in identity management & authentication systems
- inadequate protection of cyber identity
- misplaced trust in security mechanisms.

Security threats come from attackers propagating viruses, worms, Trojans, phishing, denial of service attacks and so on, which afflict today's networks and can be expected to afflict AmI networks in the future as well. Attackers can be regarded as criminals and terrorists, but government and industry may also seek to exploit AmI networks (surreptitiously or otherwise) in a way that encroaches upon our civil liberties.

Security vulnerabilities include system complexity, unexpected behaviour, inadequate reliability, the generation of false positives and insider attacks by authorised, but dishonest employees.

Additional vulnerabilities stem from individuals who are careless, lose their mobiles, forget to use security measures and/or are easily tricked. Organisations may not take adequate security measures, don't know what to protect, don't keep software up to date and/or have cost issues.

Trust in AmI networks, like trust in existing networks, may be undermined by factors including the following:

- lack of trust in underlying cyber infrastructure and other people
- identity theft
- resourcefulness of hackers & intruders
- inadequate profiling (attribution conflicts & misinterpretation of user needs)
- loss of control
- technology paternalism (machines know best)
- unpredictable system behaviour
- hijacking of an AmI system
- service denial & discrimination
- victimisation

The SWAMI consortium foresees that the *digital divide* could grow wider because of

- technological & user dependencies
- insufficient interoperability
- cost
- isolation
- AmI "technosis" (a phobia arising from the prevalence of AmI networks)
- stress
- exclusion and discrimination – unequal access & stigmatisation.

SWAMI considers that the multiplicity of threats and vulnerabilities will require a multiplicity of safeguards, some of which are technological in nature while others can be characterised as socio-economic, legal or regulatory in nature.

Technological safeguards will provide for anonymity, pseudonymity, unlinkability and unobservability. An important safeguard will be access control measures that are unobtrusive, continuous, context-dependent and provide multimodal authentication as well as the embedding of legal requirements and user wishes. They will feature artificial intelligence to catch unusual usage patterns.

Socio-economic safeguards include such features as

- open standards
- codes of practice
- service contracts
- trust marks
- privacy audits
- education
- public awareness & media attention.

SWAMI believes that the European Commission and Member States will need to take a number of actions in order to ensure the success of AmI. Such actions will relate to

- accessibility & inclusion
- accountability, audits, international collaboration, enforcement
- research proposals to identify potential privacy impacts
- guidelines for ICT research
- public procurement
- developing the legal framework to take AmI into account.

More detail on these and related issues can be found in the third SWAMI report and, as mentioned above, in summary form in the paper circulated just before the conference.

The SWAMI "Dark" Scenarios

Ioannis Maghiros

European Commission, DG JRC, Institute for Prospective Technological Studies (IPTS),
Edificio Expo, C/ Inca Garcilaso, s/n, 41092 Sevilla, Spain,
Ioannis.Maghiros@cec.eu.int

The SWAMI developed 'dark' scenarios are the centre piece of the SWAMI project methodology. The need for such scenarios stems from the fact that while foresight studies require scenarios that include an inherent bias towards presenting mostly optimistic visions of the future, reality is never so rosy and therefore there is need to consider the adverse consequences of emerging technologies. Dark scenarios are realistic although fictional extrapolations of the future highlighting potential vulnerabilities and associated threats. It is a tool to stimulate debate, to structure thinking, to facilitate 'What if' games to aid in the synthesis of realistic future plans as well as to help in raising awareness intuitively.

The SWAMI partners came up with a specific process to develop such scenarios and emphasised the need for a technology and a reality check, as well as the need for thorough legal and social/ethical analysis of the outcome. Thus, suitable scripts were developed and modified accordingly to present issues relating to individual as well as societal level concerns as well as private and public sphere concerns. There are a lot of novelties introduced by the scenario scripts however it is clear that any number of likely alternative scripts could have been used to demonstrate the issues identified or other ones that could even be more important a future challenges. One of the main aims of the SWAMI dark scenarios is to prove the need for such a process to be extended as a methodological tool related to any emerging technology before its introduction in the market place.

The main conclusions from the scenarios are that proposed safeguards ought to be holistic and context-dependent at the same time; these need to address political, economic, social, ethical, legal and technological issues and also consider stakeholder strategy and market rules. Also, it is clear that safeguards thus produced will have to be often revised as risks and vulnerabilities change as society adapts. Finally, methodologically speaking, 'dark' scenarios is a delicate exercise which is oriented not to 'high' risk areas but to everyday life and failures that are important for enhancing adoption and therefore for innovation, jobs and growth [1].

References

[1] 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., and Vildjiounaite, E. (2005). Safeguards in a world of ambient intelligence (SWAMI): Dark scenarios on ambient intelligence – Higlighting risks and vulnerabilities. SWAMI Deliverable 2. http://swami.jrc.es

The legal aspects of the SWAMI project

Serge Gutwirth, Paul De Hert, Anna Moscibroda, and Wim Schreurs

Vrije Universiteit Brussel, Faculty of Law, Law Science Technology & Society (LSTS), Pleinlaan 2, 1050 Brussel, Belgium, {firstname.lastname}@vub.ac.be

The analysis of the legal aspects of AmI started by describing the existing relevant European law. In the next step, we applied the identified legal framework to the SWAMI "dark scenarios". This exercise resulted in the identification of lacunae and problems in the existing European Information Society law. Consequently, in a third step, we moved to the development of legal safeguards addressing key pre-identified threats and vulnerabilities and policy options.

However, several particularities of the legal regulation of AmI should be highlighted.

First, the law is only one of the available sets of tools for regulating behaviour; others include social norms, market rules and the architecture of the technology (e.g., cyberspace, ambient intelligence, mobile telephony, ...) [3, 1]. On the one hand, the architecture of AmI might well make certain legal rules difficult to enforce (for example, data protection obligations, copyrights) and it might cause new problems, particularly for the new environment (spam, dataveillance). On the other hand, the architecture has also the potential to regulate by enabling or disabling certain behaviour, while law regulates via the threat of sanction. But the law can also regulate by influencing the development of the architecture.

In order to tackle the identified problems effectively, it is necessary to consider these approaches simultaneously: Should the law be adapted or modified? Should the architecture (or "code") be changed? Should the socio-economic environment and conditions change?

Second, it is certainly justified to consider the application of the precautionary principle (originally established as a legal principle for ecological problems) to ICT problems and AmI. As the impact and effects of the large-scale introduction of AmI in societies certainly spawn a lot of uncertainties, the careful démarche implied by the precautionary principle, with its information, consultation and participation constraints, might be appropriate. The application of this principle outside the scope of environmental law has been somewhat contentious. Yet, it might inspire us in devising legal policy options when, as regards AmI, fundamental choices between opacity tools and transparency tools must be made [2]. Opacity tools, on the one hand, proscribe the interference of the powerful actors into the individual's autonomy, while,

on the other hand, transparency tools accept such interfering practices, though under certain conditions which guarantee the control, transparency and accountability of the interfering activity and actors. Like other constitutional systems, Europe uses both tools at the same time. The articulation of the right to privacy (an opacity tool) and data protection law (a transparency tool) should be understood along these lines. In our opinion, most of the challenges arising in the new AmI environment should be addressed by transparency tools (such as data protection and security measures). Transparency should be the default position, although some prohibitions referring to political balances, ethical reasons or core legal concepts should be considered too.

Another particularity of the legal regulation in cyberspace is the absence of a central legislator. In Europe, the legislative powers are exercised by the Member States, though some powers have been transferred to the European Union. But some decision-making competencies have also been delegated to the independent advisory organs (children's rights commissioners, data protection authorities). And, in fact, even the technology producers are regulators of the new environments (e.g., Acrobat Reader). We thus recommend allowing all of these actors to play their respective roles, and to involve them in the policy discussion. Development of jurisprudence should also be observed. The legal profession is far from high-level abstract arguments, and tends to solve problems by focusing on concrete situations. Thus, in developing policy options, one should focus on the concrete technologies, and apply opacity and transparency approaches accordingly.

References

[1] Brownsword, R. (2005). Code, control, and choice: Why east is east and west is west. *Legal Studies*, 25(1):1–21.

[2] De Hert, P. and Gutwirth, S. (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In Claes, E., Gutwirth, S., and Duff, A., editors, *Privacy and the criminal law*, pages 61–104. Intersentia, Antwerp, Oxford.

[3] Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, 133:501–546.

Policy Options to Counteract Threats and Vulnerabilities — First Results

Background Paper for the Conference Participants

Michael Friedewald[1], David Wright[2], Ralf Lindner[1], Elena Vildjiounaite[3], Pasi Ahonen[3], Petteri Alahuhta[3], Sabine Delaitre[4], Ioannis Maghiros[4], Serge Gutwirth[5], Paul De Hert[5], Wim Schreurs[5], and Anna Moscibroda[5]

[1] Fraunhofer Institute Systems and Innovation Research, Karlsruhe, Germany
[2] Trilateral Research & Consulting, London, United Kingdom
[3] VTT Electronics, Oulu, Finland
[4] EC, DG JRC, Institute for Prospective Technological Studies, Seville, Spain
[5] Vrije Universiteit Brussel, Faculty of Law, Law Science Technology & Society, Belgium

1 Introduction

1.1 Challenges for EU Policy-Making

The definition of and provision for safeguards can be seen as critical for the rapid deployment and further development of ambient intelligence in Europe. Moreover, they are in line with those of the IST priority and the broader objectives of the Sixth and forthcoming Seventh Framework Programmes as well as related objectives stated by the European Commission, the Council and others. The Framework Programmes emphasise the importance of taking the human dimension into account in ambient intelligence. In doing so, they echo the eEurope 2005 and the i2010 Action Plans that say that Europe should have a secure information infrastructure. To that end, they identify priorities for FP6 and FP7 as including trustworthy network and information infrastructures with an emphasis on emerging technologies such as ambient intelligence. Research activities are expected to take into account the human factor in security [7, 9]. The IST 2003 report puts it even more succinctly: "Instead of making people adapt to technology, we have to design technologies for people" [8, p. 10].

SWAMI aims to formulate and consider how and to what extent it is possible or could be possible in the future to overcome the problematic implications of the dark side of ambient intelligence through the implementation of various safeguards and privacy-enhancing mechanisms, the aim of which is to ensure user control and enforceability of policy in an accessible manner and the protection of rights for all citizens in their roles (private and professional) in the Information Society.

Rather than providing a set of firm recommendations, we aim to offer a set of options as well as the description of the conditions that are at the origin of the proposed options, so that decision-makers, in exercising their political judgement and taking into account other factors, notably cost, may flexibly formulate new policies.

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

In this paper, we focus on threats and vulnerabilities to privacy, identity, security, trust and digital divide and the safeguards needed in an AmI world to deal with them. The third SWAMI report will deal with these and related matters at greater length.

1.2 Privacy

The notion of privacy is unstable, complex, difficult to fix. People's perception of privacy is context-dependent, in time and space. Our expectations of privacy may be different according to our age, gender, culture, location, family history, income, educational level and many other factors. It is no surprise that scholars understand privacy in different ways, with some arguing that autonomy and liberty are the values

behind privacy, while others contend it is intimacy, confidentiality or the control over personal information.

In the Western world, it is often assumed that most people prefer to maintain their privacy rather than giving it away. If they give up some of their privacy, they usually want something in exchange. Many people are willing to forego some of their privacy to live in a surveillance society because they attach a greater value to their security than their privacy, however they define it.

We may or may not know when our privacy has been violated. The threats to our privacy come from many different sources. If we value our privacy, it behoves us to be aware of the threats to it and to make countermeasures.

In a world of ambient intelligence, the threats to our privacy multiply. In an AmI world, we can expect to be under surveillance wherever we go. With machine learning and intelligent software, our behaviour and preferences can be predicted. Networking sensors can monitor what we are doing.

1.3 Identity

In applications ranging from electronic commerce to electronic tax filing, to controlling entry to secured office buildings, to ensuring payment, the need to verify identity and authorise access has driven the development of increasingly advanced authentication systems. These systems vary widely in complexity and scope of use.

While there are many authentication technologies, virtually all of them involve the use of personal information and, in many cases, personally identifiable information, which has raised a number of privacy concerns [19, p. 17].

A variety of identity mechanisms exist. Some of these mechanisms actually identify the person, while others authenticate a person's identity or authorise the person to undertake a transaction or have access to specified data.

As we can be identified in many different ways, so the concept of multiple identities has arisen. We may have multiple identities, which serve different purposes in different contexts – e.g., as a family member, an employee or student, a neighbour, a friend, a business associate and so on. Thus, different sets of information are associated with an individual in different contexts. Multiple identities might be better termed as a collection of partial identities.

To function in the cyber world, people need an identity or multiple identities. In some instances, we can hide behind our cyber identity, that is, to minimise the disclosure of personal information. In other instances, this may not be so possible. For example, some service providers, like the government, may require personally identifiable information, so that if we want the service, we must provide the personal data demanded by the service provider.

Hence, the individual will need to have some means to choose the appropriate partial identity to use. In many cases, she will want to avoid linkages. She will need to be able to access some identity management system that will help her to choose the appropriate identity to use in particular circumstances.

Recognising that the digital representation of identity has all sorts of ramifications, the Commission has provided funding for several projects aimed at exploring and finding ways of resolving some of these ramifications.

An AmI world will be an increasingly transactional world, where we need to identify ourselves or to use a partial identity in order to use an AmI service, most probably many times a day. In some instances, the identification or authentication process will be as a result of a conscious, deliberate decision on our part. In other instances, it will happen automatically.

With intelligence embedded everywhere in an AmI world, our identity may mutate from a collection of our attributes or a partial identity which we create to something that is created by our presence in and movement through that world. Our identity could become an accumulation of not just our attributes and identifiers, as it is today, but an accumulation of where we have been, the services we have used, the things we have done, an accretion of our preferences and behavioural characteristics. Future technologies may pinpoint our identity according to biometric combination, like the way we walk plus our facial characteristics plus manner of speaking plus how we respond to certain stimuli. Needless to say, this kind of identification could give rise to a host of security, privacy and trust issues.

1.4 Security

With the growing dependency on computer systems, security becomes a more important issue than ever. Threats to security in an AmI world may well be greater in number and ramifications than those posed to today's networks. The main reasons for this are, on the system side, the sheer increase in the number of computers and of network transmissions, the convergence of different networks, the growing complexity of systems and diversity of versions. Second, the growing dependency on computers and blurring of boundaries between professional and personal use of them, on the one hand, and lack of special education of users of these complex systems, on the other hand, present big challenges to security. People who have a low degree of technology literacy are unlikely to configure well the security settings of their personal devices. Third, opportunities for earning money via computers will grow in an AmI world. Some of these opportunities such as e-commerce, selling games or mobile services will be legal; others, such as phishing or data laundering, won't be. With intense competition between service providers, some new software will not be validated properly before being put on the market. Some threats and vulnerabilities will compromise security and trust.

The main drivers of security threats and vulnerabilities are (1) the lack of awareness or attention on the part of some users with regard to security settings and updates, (2) insufficient attention given by software producers to make sure that their security measures are intuitive and user friendly and by their not undertaking sufficiently rigorous testing of their software products (thorough testing of complex systems is a complex and expensive undertaking) and (3) the new opportunities for remote crimes.

1.5 Trust

Digital computing technology increasingly comes to provide mediation between human actors and the world. As such, these technologies structure, constrain and enable our engagement with and experience of the world [16]. Increasingly, our life is intertwined with or related to digital technology. In order to put digital technologies to satisfactory use, and in order to have a convenient and useful interaction with and through technology, trust is a fundamental precondition. The often-reported lack of trust in e-commerce demonstrates that insufficient trust can lead to users staying away from a technology altogether [11, 18].

A precursor of trust is the assumption of risk. Hazards abound in late-modern society, fundamentally changing and deepening our need for trust. Had we not trust in much of the apparatus of late-modern society, we would not be able to act at all; we would be tied to our bed for fear of venturing out into a society permeated by seemingly inescapable danger. Trust can be conceptualised as "a willingness to enter into interaction under the face of uncertainty" [21].

We no longer exist in close-knit communities, allowing for deep knowledge, traditions and the visibility of the geographically co-located other [10]. Trust is a necessary feature of life in contemporary societies, as we are surrounded by various kinds of hazards, and as a time-space distance exists between actors and expert systems that help us to manage the risks.

1.6 Digital Divide

The digital divide basically refers to the gap between those communities or groups that have access to the Internet, ICTs or any emerging digital technologies and those that do not, as well as to the disparities regarding the competencies to use them or their respective learning capabilities. The digital divide is a societal, economic and political issue, all rolled into one. It raises several types of problems and difficulties involving costs, culture, organisation, education, acceptance, adaptation, geography and demographics.

Because of its envisioned user friendliness and intuitive aspects, AmI technology clearly has the potential to bridge some current gaps of the digital divide, but, at the same time, this technology could also broaden the digital divide with regard to unequal access, quantity and quality of use.

In SWAMI's deliverable D2, scenario four "risk society" [26] highlighted this threat in terms of social and organisational aspects. It shows that ambient intelligence services are not automatically becoming public utilities for the benefit of the whole society. In fact, the big investments needed for installation of an AmI infrastructure may result in an economic rationale to mainly offer private – possibly expensive – goods and services, leading to the exclusion of those groups that could actually benefit most from such services. It is by no means self-evident that AmI services will become as widespread as mobile communications are today, especially in less developed regions. Moreover, within the digital divide issue, technological aspects and questions of media competence and technology literacy are closely interrelated.

2 Threats and Vulnerabilities

2.1 Concept and definition

Unless adequate safeguards are implemented, the diffusion of AmI applications will entail negative side effects and create risks, which, if not addressed, may jeopardise the potential economic and social benefits of the technology. Prior to the formulation of appropriate safeguards and policy options, a better understanding of AmI's unwanted consequences needs to be developed. Analytically, the potential dangers associated with AmI systems can be differentiated into threats and vulnerabilities.

SWAMI's use of these terms is based on definitions presented by the Special Interest Group 2 "Security and Trust" of the Wireless World Research Forum [15, p. 14]:

- A vulnerability is a flaw or weakness in a system's design, its implementation, or operation and management that could be exploited to violate the system and, consequently, cause a threat.
- A threat is the potential for one or more unwanted consequences caused by a circumstance, capability, action, or event that could be harmful to a system or person. Threats can be caused naturally, accidentally or intentionally.

2.2 Privacy

Hackers and malware

When we progress to an Internet of things and fourth generation mobile networks, with heterogeneous devices able to access interconnecting networks, we should assume that hackers will still persist in trying to break into networks with malicious intent ranging from the nuisance level to serious harm to critical infrastructure.

Malware — spyware, adware, viruses, Trojans, worms, denial of service attacks – have been unfortunate features of daily life on the Internet and, lately, with advanced mobile phones. Often, malware is aimed at uncovering and exploiting personal and confidential data. Can we expect a cleaner future in a world of ambient intelligence? Or will new forms of malware be created in order to exploit an Internet of things and fourth generation mobile phones? Clearly, we should assume that malware will be a part of our embedded future just as it is daily phenomenon today. We should assume that our AmI environment will be under attack not only by criminals, but also by industry and government.

Function creep

Function creep occurs whenever data are used for a purpose other than that for which they were originally collected. AmI will give great impetus to function creep. An AmI world is distinguished not just by ambient intelligence, but also by the interoperable networking of heterogeneous devices. It's been said that whatever can be

linked together will be linked together, and therein lie the opportunities and temptations for function creep. Some have suggested that (precautionary) impact assessments should be made of new technologies before they are developed and deployed in order to build in privacy safeguards. But some technologies may be used for new applications not foreseen until after they are deployed.

Security and surveillance

Surveillance is increasing in the streets, buses, underground, shops, workplace, and on the motorways. In some cities, such as London, it is now almost impossible to go outside your home without coming under surveillance. While AmI technologies will offer benefits in terms of enhancing security, they will also present greater threats to our privacy and to our security. AmI devices such as implants or technologies that monitor our physiological condition and behaviour could well make our society more secure, particularly if they enable law enforcement authorities and intelligence agencies to take preventive measures. Preventive actions by the police are featured in the Spielberg film, Minority Report, but is this the kind of society we want? In any event, more control in order to prevent criminal acts, detect offenders and punish them may be counterproductive for society as a whole. In 1968, the philosopher Heinrich Popitz wrote a classic text on the "preventive effects of nescience" [25] in which he argues that too much (precautionary) knowledge destabilises society, leads to a climate of distrust and finally to more instead of less crime.

Profiling

Security expert Bruce Schneier has pointed out flaws with profiling schemes. "Profiling has two very dangerous failure modes. The first one is ... the intent of profiling ... to divide people into two categories: people who may be evildoers ... and people who are less likely to be evildoers... But any such system will create a third, and very dangerous, category: evildoers who don't fit the profile... There's another, even more dangerous, failure mode for these systems: honest people who fit the evildoer profile. Because actual evildoers are so rare, almost everyone who fits the profile will turn out to be a false alarm. This not only wastes investigative resources that might be better spent elsewhere, but it causes grave harm to those innocents who fit the profile... profiling harms society because it causes us all to live in fear...not from the evildoers, but from the police...." [28].[1]

Sharing of personal data between companies and government

In an AmI world, it is likely that sharing of personal data will be even more prominent than it is now. This is because many organisations will be involved in building the

[1] George Clooney provided us with a recent reminder of this in his recent film, Good Night and Good Luck, about Joe McCarthy, the US senator, who in the early 1950s professed that he was making America more secure by exposing Communists and their sympathisers, when in reality he was instilling fear and paranoia across society.

integrated networks, products and services distinguishing an AmI world. As many organisations bring their particular expertise and competencies to building these networks, it is likely that many of them will want to share user data. Hence, we can expect that such activity will further diminish the limited privacy we enjoy today.

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

Lack of public awareness about privacy rights

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

Lack of enforcement and oversight of privacy rights

Some of our personal data are held by the governments and organisations in our own countries, while some of the data may be held in other countries. Some countries may have legislation or regulation that affords relatively good protection of our privacy, while others may have regimes that offer no protection whatsoever. No matter what the best of the legal regimes say, the complexity of the regulation, incomplete enforcement and sometimes even conscious decisions by businesses and governments not to comply with the rules render legislation ineffective [12].

Erosion of rights and values

The erosion of the right to privacy in the past century has been subtle, incremental, gradual and as relentless as technological advance. In today's surveillance society, where our personal data are not secure and are mined, monitored and captured, people have surrendered the right to be let alone in the interests of greater security. But there are questions whether it has led to greater security, questions that are unlikely to be adequately answered before the widespread deployment of AmI networks in the near future. We should assume encroachments upon our right to privacy will continue in the AmI-enabled future.

Uncertainties about what to protect and about the costs of protection

Just as privacy is an unstable notion, so it is almost impossible to know what to protect in all contexts, especially in view of the capabilities of data mining and powerful software that can detect linkages that might not otherwise be apparent. In addition, people's views of privacy keep changing. With the emergence and deployment of AmI networks, the amount of data that can be captured from all sources will expand exponentially by many orders of magnitude. Hence, the cost of providing 100 per cent privacy protection may be prohibitive and unrealistic, even if there were some consensus about exactly what it is we wish to see protected.

Uncertainties about the economic costs of privacy erosion

There have been few studies aimed at analysing the value of privacy, either from a corporate point of view or that of the individual.

Lax security

One of the most serious vulnerabilities facing those who care about their privacy is the lax security put in place to protect personal data and the privacy of communications.

Government and industry are less than forthright

So many people and organisations hold personal data about us, it is virtually impossible to know who they are, let alone to keep track of what they are doing with our data, whether the data they hold are accurate, and how such data may change, be added to, deleted or amended — even though, according to data protection legislation, all these data should be available to the data protection authorities and should be provided to the individuals concerned (at least in Europe). Although these obligations exist, their efficacy has been undermined by the bad faith of some private sector data controllers and because enforcement has not been rigorous.

2.3 Identity

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

Identity theft

Identity theft is one of the fastest-growing white-collar crimes. Despite the prevalence of identity theft, prosecutions are rare. One study has said that an identity thief has about a one in 700 chance of getting caught.

It is an open question whether ambient intelligence will increase or decrease opportunities for identity theft and fraud. With orders of magnitude of more personal information generated in an AmI environment, one might not be too hopeful that the problem will go away. On the other hand, if some privacy-enhancing technologies, like those proposed in the PROGRESS[2] Embedded Systems Roadmap or in the PISA[3] and PRIME[4] projects, become widely available, the consumer might have better defences against at least some forms of identity theft.

[2] PROGRESS is the acronym for PROGram for Research in Embedded Systems and Software. The roadmap can be found at http://www.stw.nl/progress/ESroadmap/index.html

[3] PISA is the acronym for Privacy Incorporated Software Agent. http://www.pet-pisa.nl/pisa_org/pisa/index.html

[4] PRIME is the acronym for Privacy and Identity Management for Europe. http://www.prime-project.eu.org

Function creep

The growing awareness of identity theft has prompted many businesses to require customers to provide identification information, especially online and over the telephone. In attempts to minimise the risk of identity theft and fraud, businesses may be increasing risks to our privacy.

The creation of reliable, inexpensive authentication systems will invite function creep. As AmI becomes pervasive, at least in developed countries that can afford such networks, the opportunities for supplementing basic identifier data will surely grow.

Exploitation of linkages by industry and government

Even among those who understand the benefits of partial identities, it will be miraculous if they can avoid usage of at least one attribute across two or more partial identities. An AmI world will be highly networked with linkages between different networks. Hence, where today it is possible to have multiple partial identities that correspond to our different roles in society — as neighbour, employee, student, etc. — AmI will facilitate linkages between these different partial identities leading to a great increase in their integration.

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

Identity management systems are subject to many of the attacks common to other Internet or computer-communications-based systems, such as hacking, spoofing, interception and denial of service. There's no reason to think these sorts of attacks that plague us today are likely to go away in an AmI world.

Authentication may intrude upon privacy

A US National Research Council report has warned that authentication technologies could intrude upon privacy in different ways. Authentication methods may require contact with or close proximity to the body, potentially raising concerns under the "bodily integrity" branch of privacy law. Authentication may introduce new opportunities to collect and reuse personal information, intruding on "information privacy". They may be deployed in a manner that interferes with individuals' "decisional privacy" by creating opportunities for others to monitor and interfere with personal activities. They may raise new opportunities to intercept or monitor an individual's communications, revealing the person's thoughts and the identities of those with whom he or she communicates [19, p. 63].

Complexity of identity management systems

Governments and industry have been developing a multiplicity of identity management systems with the intent of putting more (or virtually all) of their services online

or, in the instance of the rationale for national ID cards, for combating fraud and terrorism.

The multiplicity and complexity of such systems offers a possible foretaste of what identity management could become like in an AmI environment, when there will be many more systems, networks and services on offer.

The snag with the growing complexity of computer communications systems, including those that will form the backbone of AmI networks, is that vulnerabilities increase with complexity. Experience has taught that systems — and, in particular, complex systems like networked information systems — can be secure, but only up to a point. There will always be residual vulnerabilities, always a degree of insecurity [27, p. 119].

Failures in identity management and authentication systems

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

Security expert Bruce Schneier has said that it doesn't matter how well a system works, what matters is how it fails. No matter what their merits may be, if identity management, authentication and authorisation systems generate a large number of false positives, they will be regarded as failures.

Problems like this could be reduced in an AmI world if the various AmI networks generate so much data about the individual that the individual is virtually unmistakeable. But if we arrive at that situation, the capture and analysis of so much information reduces the very protection of privacy that identity management systems are supposed to support.

Inadequate protection of personal cyber identity/ies

Today cyber citizens often use the same password or ID over different websites and systems. The bits of yellow notes stuck on the side of computer screens with passwords written down undermine the point of having passwords. Unconsciously or not, most cyber citizens today do not take adequate care to protect their identity or partial identities. Some of the privacy-enhancing technology schemes that are being considered for today's cyber world and that of the AmI world may help reduce this problem, but it is unlikely to go away.

Misplaced trust in security mechanisms

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

law enforcement authorities, we may be forced to rely on (to trust) the adequacy of security mechanisms, of others' privacy policies.

2.4 Security

Security threats and vulnerabilities fall into two major groups:

- First, vulnerabilities from unforeseen system behaviour or failure due to internal complexity. Complex systems usually cannot be tested in all possible configurations and situations, thus they might have many internal problems. These system errors may be caused by incompatible system hardware components or software versions after a system upgrade, programming errors, poor performance of chosen communication protocols, too low or too far a range of wireless transmission or insufficient reliability of critical components.
- Second, attackers (who exploit the above-mentioned system weaknesses and flaws) pose threats when they try to intrude upon the system to engage in identity theft, to intercept communications, to change contents or software code for their own benefits, or to find valuable physical objects.

  Both groups of threats can be further categorised as follows:

Threats to the primary operation of a system

A threat to disrupt the primary operation of a technical system or even to destroy it can be realised by exploiting internal system weaknesses. For example, in AmI health care applications, when a patient's personal device is connected to the hospital network in an emergency (in order to acquire the health data history of the patient who has been in an accident or other untoward event), reconfiguration of the system may be required for interoperability, and this reconfiguration can disrupt operation of the personal device. Or the personal device may have viruses, which are transferred to the hospital's AmI system along with the patient's data. Another common problem is that gaming applications often consume a lot of system resources and users are often encouraged to upgrade to newer versions or to install new pieces of hardware. But these upgrades may create compatibility problems and harm other functionalities of a personal device. Similarly, upgrading a factory automation system might decrease its performance dramatically due to incompatibility of different components.

Another security weakness might emerge if a personal device becomes too busy to process a large number of incoming messages (e.g., sorting messages according to the user's preferences) or to manage its other tasks. Proper prioritising of device tasks would help, but setting priorities is an additional burden for the user. Similarly, if too many wireless messages are transmitted, some smart objects with limited resources (like keys with an embedded hardware module which could help their owner to find them) can miss the only important query from the key owner and remain untraceable. Even worse, operation of pacemakers or implants can be hindered by intensive wireless communications between smart devices.

Hackers will continue to pose a threat to the operation of a system. Many networks are vulnerable to denial-of-service attacks and this may well be true of AmI networks too. Security flaws may allow software code to be replaced or modified so that the system no longer performs as it was intended. Competition between service providers might stimulate development of viruses that change user preferences in such a way that only products of certain brands get through the filter. Disruption of traffic control systems could lead to chaotic changes in traffic priorities.

Threats to physical integrity

Threats to the physical integrity of the home and property of the user can be realised by exploiting internal system weaknesses in ways such as the following: with the growing pervasiveness of AmI "little helpers", users might not care as much as today about the operation of home appliances (switching off the stove, adjusting the heating, closing the windows and doors, etc.). As a result, a system failure in any of these appliances could cause a fire due to overheating, water damage due to open windows or extra payments for heating or water consumption.

Improper access to home control systems via the AmI network could enable criminals to cause a fire or gas leakage remotely, to check and steal valuables in the home or in the car.

M-commerce applications and phishing could lead to identity theft with all its consequences.

Customer profiling may result in customers paying more for services, especially if they are not aware of other options or do not want to be tracked. If a shop owner can use an AmI system to determine whether a particular customer is wealthy, then the shop owner might only suggest the most expensive items for purchase. Insurance companies might also use customer profiling and impose higher premiums for those users whose profiles suggest that they present higher risks.

Threats to health and life

Threats might arise because of internal AmI system flaws in life-critical applications, while the dependency on these applications will be growing. For example, any failure in health monitoring or in a health care application (an error in diagnosis, a failure to transfer personal data at the right time, a failure to remind a patient to take his medicine, disturbances to pacemakers from radio interference) may create a serious risk to an individual's health and life. Similarly, any failure in traffic control or warnings about approaching cars will create the risk of an accident. Failure to switch off the gas or fire could be hazardous and life threatening. A failure in an industrial system may be the cause of a dangerous accident.

Some threats will arise as a result of malicious actions such as intentional disruption of life-critical applications (e.g., by means of a denial of service attack on a health monitoring network or a traffic control system so that they are unable to generate an alarm). AmI could be used to remotely carry out a murder. Leakage of personal location data may result in a kidnapping or terrorist attack. Criminals and

terrorists could spoof an AmI biometric access control system in order to cause harm to others. Someone could use AmI systems in order to humiliate another through disclosure of personal secrets, which may result in the victim's committing suicide.

Threats to personal dignity and general annoyance

Threats to personal dignity may not lead to such grave consequences as the previous ones, but they are likely to be more frequently encountered in real life. Such threats could come about as a result of flaws in an AmI system, such as a lack of system intelligence (inability to identify sensitive data in a specific situation) which leads to an inappropriate disclosure of personal data, frequent and annoying alarms, insufficiently high performance of algorithms (poor encryption or slow decryption or errors in person recognition), ineffective anti-virus and anti-spamming software, losses of important data due to system complexity or viruses.

These threats can be realised by viruses, spamming and denial of service as well as by surveillance by government, insurance companies, employers, family members, neighbours, etc. Such threats could be realised by changing program code or reconfiguring the system in such a way that the user does not know how to get back to normal system operation.

2.5 Trust

One of the chief inhibitors to the growth of public acceptance of the Internet for human interactions (commercial or otherwise) has been the lack of trust in the underlying cyber infrastructure and in other people whom we meet through that infrastructure. Incidents of massive identity theft from otherwise internationally trusted financial institutions, the never-ending resourcefulness of malicious hackers and intruders, have increased the apprehension and uneasiness of the general public vis-à-vis the Internet and the Web — and there is strong evidence that this will apply even more to ambient intelligence services in the future. It is a challenge to change this climate not only at the level of interactions among human agents (commercial or otherwise) through the use of the cyber infrastructure, but also among human and software agents.

Inadequate profiling

As the AmI vision is geared towards a user-driven approach, one of the key means of meeting the users' individual needs is personalisation. Based on constructed profiles, AmI systems are enabled to respond to the users' needs — or at least what is assumed to be their needs inferred from the interpretation of the collected information. Problems of inadequate profiling can occur with regard to two main situations: attribution conflicts in case of numerous users and misinterpretations of users' needs.

Multi-users

In the case of incorrect attribution, two or more users are concurrently present in an AmI environment. The users' profiles, actions and preferences may not necessarily be congruent [29, p. 12]. If profiles are completely or even partially incompatible, conflicts over shared services and resources might occur. A possible solution is to average out the disputed profile parameters. However, in many areas of daily life — for example, with regard to different music styles — such simple mathematical remedies are not feasible.

Misinterpretation of needs and insufficient expression of preferences

The quality of a personal profile depends both on the scope and depth of the input data as well as on the suitability of the data processing routines. However, the profiles developed on the basis of the collected data can merely represent — at best — approximations of the actual user preferences. Most dimensions of human self-expression include implicit, intangible, subtle and fuzzy forms, making it — at least for the time being — impossible to reconstruct them adequately. In short, linking observable behaviour to an individual's intentions is problematic and prone to misleading interpretations – a challenge, of course, faced by every developer of an "intelligent" system.

These considerations on profiling are not intended to support the conclusion that profiling is to be dismissed per se. Instead, a better understanding of the innate limits to the construction of user profiles should entail a heightened awareness for the necessity to implement adequate provisions that help to reduce undesirable side effects.

Loss of control

"Technology paternalism"

Technology paternalism [31] arises in those instances in which machines decide autonomously and in an uncontrolled manner on behalf of and supposedly in the best interests of a user. Technology effectively infringes upon individual liberty if no easy-to-use and convenient override options are available and the user does not want to comply with the settings of an AmI system – for whatever reason. The possible drawbacks from technology paternalism can range from constant irritations to fundamental distrust in AmI, possibly leading to a deliberate decision to avoid AmI systems as far as possible.

Unpredictable or unexpected system behaviour

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

Due to the technology's complexity or the different conception that program developers and users have of the proper use of the information systems, many users may conclude, based on their experience, that they cannot rely on the systems as expected. Moreover, as dependency on such systems increases, the potential harm, which could result from a misjudgement of system behaviour, also rises.

"Hijacking" of an AmI system

In the case of a hijacked AmI system, the user's loss of control is not caused by default system settings. Instead, the situation clearly depicts a deviation from normal procedures due to malicious or criminal interference. Once hackers and attackers gain full or even partial control over an AmI system, they might be able to re-adjust personalised settings and extract sensitive information stored in databases in order to use them illegally. The potential consequences for trust in AmI applications are more than obvious.

Denial of service and discrimination

Denial of services and incidents of discrimination originate in procedural rules imposed by service providers – either in their own right or in compliance with regulations established by public bodies. In both cases, specified profile characteristics have to be met by the individual if he or she desires access to certain services or privileges.

Furthermore, problems of service denial might not only occur in instances in which a user's profile does not match the required criteria (e.g., income, age, health record or other aspects of the personal data history), it is also conceivable that an individual's deliberate decision not to make available certain elements of personal data will result in undue exclusion.

Situations in which discriminatory refusals of services can take place are characterised by asymmetric relationships in which one party is obliged to comply with standards defined by the other party. Two main realms of discriminatory practices due to allegedly insufficient profiles can be distinguished:

Civil security

Based on security concerns, users have to provide personal information as a prerequisite to gain access. From the citizen's perspective, two problems may arise. One is the difficulty to discern whether a certain access restriction is based on public regulations or the service provider's own rationales, raising questions regarding the legitimacy of the imposed measure. The other is the refusal of services which can be due to either insufficient interoperability of information systems or, for instance in the case of individuals from less developed regions, the absence of personal profile data in the first place.

Profit interests

Apart from pure security motives, market and profit considerations can be at the heart of access rules. For instance, customers might be coerced into disclosing sensitive personal data if they want to enjoy certain privileges or services (e.g., special insurance premiums or rebates). Moreover, if a customer deliberatively decided not to comply, possibly for perfectly legitimate reasons, a service provider might respond by limiting its own liability.

Victimisation

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

2.6 Digital Divide

A broad range of threats and vulnerabilities relate to the digital divide issue. Among the most important ones are different aspects of dependency and exclusion / discrimination.

Dependency

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

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

Insufficient interoperability

This vulnerability is caused by technological dependency and has two main aspects: spatial and temporal. The spatial aspect concerns the lack of interoperability between geographical entities. In order for AmI to function across borders, different regions and countries need to use technologies that interoperate. Further harmonisation of

standards with varying degrees of geographical scope will be needed (e.g., EU, international). Some countries, however, will not be able to afford to fully comply with the standards created in developed countries. Solutions to overcome the potential divides based on insufficient interoperability need to be envisaged.

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

Cost effectiveness

On the one hand, the drive towards cost saving could give a boost to the implementation of AmI, but on the other hand, maintenance and updating could be much more costly than initially expected. Therefore, high costs may be the source of unwanted consequences, emphasising the digital divide between countries but also within societies.

Isolation

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

"AmI technosis"

The disruption of social behaviour due to addiction might be caused by a user's dependency on new means of communication and particularly by the ubiquity of these applications made possible by AmI technologies.

Stress

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

Exclusion and discrimination

Unequal access

AmI technology has the potential – due to its foreseen user friendliness and intuitive aspects – to bridge some aspects of the current digital divide. On the other hand, AmI technology could also amplify other aspects of unequal access and use. This threat has technical as well as social and organisational dimensions. There are no guarantees that ambient intelligence services will be public utilities to the benefit of all.

Stigmatisation

Because many AmI technologies and devices will need profiling data in order to provide users with the expected and suitable services, profiling data will proliferate within the AmI networks. The misuse of profiling data may exacerbate exclusion and discrimination. The heavy presence of such data may make the common origins of stigmatisation (cultural, ethnic, socio-economic) more obvious and reinforce existing or generate new forms of discrimination.

3 Safeguards

It is clear from the multiplicity of threats and vulnerabilities facing our notions of privacy, identity, security, trust and digital divide that a multiplicity of safeguards will be needed to protect them. The following safeguards are grouped into three categories: technical, socio-economic and legal.

3.1 Technological Solutions

Currently most of the research on privacy protection is concerned with user privacy in network applications and with security of personal devices, and addresses privacy protection in the context of current technology [14, 5, 6]. The main privacy-protecting principles in network applications have been stated to be

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

The main difference between existing network applications and emerging AmI applications is twofold:

First, in the former case, the user nominally has some understanding of which data about him are collected, and has some means to restrict data collection. In the latter case, an environment full of numerous invisible sensors makes it difficult (if not impossible) for the user to understand and to control data collection and to achieve unobservability, anonymity and pseudonymity.

A second important difference between existing network applications and emerging AmI applications is that neither mobile devices nor web usage penetrates through such strong privacy-protecting borders as walls and the human body, while physiological, video and audio sensors, proposed for AmI applications, have much stronger capabilities to identify a person and to reveal personal activities and feelings.

Consequently, future AmI applications require stronger safeguards, and many of them are not yet fully developed. We propose research directions for developing privacy protecting safeguards in future AmI settings.

Minimal data collection, transmission and storage

The less information about users that exists in AmI systems, the less personal data AmI systems can disclose. AmI applications will undertake two main actions: data collection in the user's physical location by sensors and by logging user-computer interactions; data transmission and data storage either in a personal device or in a remote database. Care should be taken to minimise system knowledge about users at any stage of any action. The goal of the minimal data transmission principle is that data should reveal little about the user even in the event of successful interception and decryption of transmitted data. Similarly, the principle of minimal data storage requires that thieves don't benefit from a stolen database and decryption of its data. Implementation of anonymity, pseudonymity and unobservability methods help to minimise system knowledge about users at the stage of data transmission and storage in a remote database, but not in cases of data collection and storage with a personal device (which collects and stores the device owner's data) or video storage.

The main goals of privacy protection during data collection are, first, to prevent linkability between diverse types of data collected about the same user; and second, to prevent surveillance by means of spyware or plugging in additional piece of hardware transmitting raw data. These goals can be achieved by careful selection of hardware, by increasing software capabilities and intelligence (so that data can be processed in real time) and by deleting data as soon as the application allows.

In practice, it is often difficult to determine what "minimally needed application data" should be, moreover, that data can be acquired by different means. Maximising software capabilities is needed for minimising storage of raw data and for avoiding storage of data with absolute time stamps. We suggest this safeguard in order to prevent accidental logging of sensitive data, because correlation of different kinds of data by time stamps is relatively straightforward.

Security

In this section, "security" is intended to mean the protection of data and software from malicious actions (e.g., data theft, modification of program code, etc.). In some instances, security can endanger privacy. For example, surveillance of all people in a country may increase security by making it more difficult for criminals to act or terrorists to go undetected, but such a level of surveillance will undoubtedly be invasive of privacy and have a chilling effect on civil liberties and personal freedoms.

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

Privacy protection in networking

Data transfer in AmI applications takes place between remote locations, as well as between diverse sensors in a smart space and between devices which belong to a personal area network (PAN), e.g., sensors attached to a human body in different placements or to personal belongings. In all transfers, the data should be protected by security means from malicious actions such as interception, data modifications and denial of service and by access control methods (see the next section). When data are transferred, anonymity, pseudonymity and unobservability should also be provided. The ways to do it include, first, methods to prove user authorisation locally and to transmit over a network only the confirmation of authorisation; second, methods of hiding relations between user identity and actions, e.g., by distributing this knowledge over many network nodes; third, special communication protocols which do not use a device ID or which hide them.

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

Authorisation and access control

Access control policies and procedures are designed to ensure that only those properly authorised have access to specified data, to guard against external hackers and rogue employees. Access control, in the sense in which ISO uses the term in its 17799 standard, refers to measures taken within an organisation to ensure information security.

ISO 17999 states that "the use of personal or privately owned information processing facilities ... for processing business information, may introduce new vulnerabilities and necessary controls should be identified and implemented" [17, p. 11]. By implementing such controls, organisations can, at the same time, achieve both organisational security and personal data protection. It also suggests that an appropriate set of procedures should be defined for information labelling and handling, in accordance with the classification scheme adopted by the organisation. These procedures should cover information assets in both physical and electronic formats, as well as different activities, such as copying, storage and transmission. To provide for employees' privacy, organisations complying with the ISO 17799 should adapt their classification scheme according to the monitoring and privacy protection guidelines.

In AmI networks, access control policies and procedures will most probably be needed outside the organisation as well, in the embedded world of networked sensors and actuators, 4G devices and so on. Thus, those who are authorised and whose identifiers or attributes can be authenticated will have access to some AmI services and networks (but perhaps not others), while those who cannot be authenticated won't have access.

The traditional understanding of the term "access control" involves granting a person the right to log in and to have access to certain data or enter an office. Proper

methods of access control will also be needed in different future AmI applications. Physical access control is required in such applications as border control, airport check-ins and office access. Access control is required for computer login and personal device login and such network applications as mobile commerce, mobile voting and so on. There is a growing need to employ reliable authentication methods instead of passwords commonly used today.

Currently, strong authentication procedures (such as iris or fingerprint recognition) have the drawback that the trust in them is so high that if an impostor succeeds in being verified once, he can do whatever he wants. Reliable authentication is one that has low error rates and strong anti-spoofing protection. We suggest that really reliable authentication should be unobtrusive, continuous (that is, several times during an application-dependent time period) and multimodal (it is more difficult to spoof several biometric modalities than the only one). If a car lock can only be opened by the car owner's fingerprint, there is a danger that criminals will either produce a faked fingerprint or, worse, cut off the owner's finger. However, if authentication of the owner continues inside the car (e.g., by iris scan, voice or face recognition or other biometrics), the impostor will be discovered sooner or later. Consequently, the incidence of car theft could be reduced (in theory).

Unfortunately, research on continuous multimodal access control has been somewhat limited. It is also worth noting that most access control methods don't help against an authorised but dishonest person stealing data. Use of artificial intelligence safeguards (see below), however, could help in such cases.

In addition to multimodal authentication, methods should be developed for reliable unobtrusive authentication (especially for privacy-safe unobtrusive authentication). The current state of the art in authentication is such that reliable authentication requires explicit user effort, while unobtrusive authentication is not reliable. Moreover, most efforts in unobtrusive authentication are devoted to face and voice recognition, which could threaten privacy. It is also possible (although not so reliably) to verify the user by patterns of mouse and keyboard usage [1], by weight, height, body fat percentage [3], by gait [22, 2] and probably also some other features. Multimodal verification by many unobtrusive modalities together should increase reliability, while being more privacy-safe. Both unobtrusive privacy-safe biometrics and multimodal biometric fusion are, however, fairly young research areas, and not mature yet.

Unobtrusive authentication should allow greater security because it is user-friendlier. Most people are not willing to use explicit authentication frequently, which reduces the overall security level, while unobtrusive authentication can be used continuously. For example, if a person works with large databases of sensitive data, continuous unobtrusive authentication (e.g., by patterns of mouse usage) would prevent a situation when an impostor succeeds in spoofing the system once (e.g., with faked fingerprint and stolen implant) and after that gets full access to sensitive information. Continuous unobtrusive user verification (e.g., by voice and gait) is needed for protection of personal devices. Currently, personal devices (especially mobile phones) are used unprotected for a long time after a user has switched a device on, due to users' unwillingness to use explicit verification protection frequently (such as typ-

ing a password or giving a fingerprint) and due to the fact that a phone needs to be switched off before it requires user verification.

Access control should also be made context-dependent, e.g., by requiring more reliable authentication if a user spends more money than usual (above a predefined threshold), or if a mobile device user is in a foreign location than if he is alone at home. Such context-dependent authentication is not yet mature for real life use, especially since current authentication methods are mainly explicit and not really multimodal.

Recently, the term "access control" has also been used in the context of checking which software is accessing personal data and how the personal data are processed. This should be achieved by developing ways to express legal requirements and personal user wishes in machine-readable rules and by embedding these rules into personal data in such a way that they cannot be ignored or bypassed (similar to how digital rights management methods should prevent illegal copying of files).

An example of this form of access control is the Personal Well-being Assistant envisaged by the PROGRESS Embedded Systems Roadmap. The individual user would be able to control or set the features he or she wants, including his or her personal privacy settings, which could vary depending on the context or time or type of transactions to be performed. Conceptually, the notion of a PWA as an interface with the ambient intelligence environment with "tuneable" privacy and security levels is an interesting potential safeguard. Even better, the PWA would be able to advise users if they weren't sure what level of privacy protection would be appropriate in a particular context.

The PWA and other similar privacy-enhancing technologies could be regarded as anonymisers, the purpose which is to ensure that, in any given transaction, no or minimal information could be linked to our identity. The information to be collected in any transaction should be limited to what is necessary to support the transaction. The snag for our law enforcement authorities is that anonymisers may help to prevent identity theft and fraud, but they can also be used by criminals to cover up illegitimate activities.

Generic architecture-related solutions

The main goal of high-level application design is to provide an appropriate level of safeguards for its level of threats. This can be achieved by proper data protection (e.g., by encryption or by avoiding usage of inexpensive RFID tags which do not have access control to their ID) and by minimising the need to protect data (e.g., by broadcasting of advertisements so that each personal device can select the most interesting ads for its owner, instead of revealing personal preferences by querying shops). High-level application design should also consider which level of technology control is acceptable (i.e., is the application smart enough to do anything autonomously or to make proactive suggestions) and provide easy ways to override automatic actions. High-level design should also take care of thorough testing of AmI systems, because with a diversity of software and hardware providers and with the growing complexity

of systems, the possibility of something unpredictable happening increases dramatically.

Still another goal is to consider how the user can escape from using AmI systems in such a way that it is not harmful to him. For example, currently it is socially accepted that mobile phones are not always with their owners (e.g., the owner can forget or lose the phone). How such freedom can be achieved in a future of smart tiny devices embedded into objects (such as clothes, watches and walls) is an open question. Another point to consider is the trade-off between device capabilities and price. For example, small screens present problems to security and privacy protection, because configuring security settings and privacy polices is more complicated. Similarly, advanced antivirus and advanced reasoning algorithms can be costly and can require more memory. However, they are important for privacy protection.

Artificial intelligence safeguards

To some extent, all software algorithms are artificial intelligence (AI) methods, for example, machine learning and data mining are traditionally considered as belonging in this area. In the context of this paper, however, AI safeguards are methods of very advanced reasoning capabilities. Although AI solutions are not yet mature, research on AI methods is taking place. Many privacy threats appear because reasoning capabilities and intelligence of software do not grow as fast as hardware capabilities (storage and transmission capabilities). Consequently, the development of AI safeguards should be supported as much as possible, especially because they are the main means of protecting people from accidental, unintentional privacy violation, such as disturbing a person at the wrong moment or recording some private action. For example, memory aid applications could automatically record some background scene revealing personal secrets or a health monitor could accidentally send data to "data hunters" if there are no advanced anti-spyware algorithms at work. Advanced AI safeguards can also serve the goals of access control and anti-virus protection, by catching unusual patterns of data copying or delays in program execution.

Recovery means

It seems quite probable that losses of different kinds of personal data will happen in future, just as identity thefts happen now. In the future, however, losses of personal data will be more noticeable due to the inevitably growing dependency on AmI applications. Consequences of data losses can cause problems in personal relations, work discrimination, financial matters or even cause death. Recovering from some data losses could be impossible or require other than technological methods, e.g., legal methods. Nevertheless, some problems can be solved by technological means. For example, in the case of theft of somebody's biometric data, there should exist means to replace compromised biometrics with another authentication method (other biometrics, tokens, etc) everywhere (in all credit cards, in all office/ home/ car locks, etc), and to do it quickly and effortlessly for the person, possibly via networks.

Another problem, which could be solved by technological means, is recovery from the loss of or damage to a personal device. If a device is lost, personal data contained in it can be protected from strangers by diverse security measures, such as data encryption and strict access control. The user should not need to spend time customising and "training" a new device (so that denial of service does not happen); instead, the new device should itself load user preferences, contacts, favourite music, etc, from some back-up service, probably a home server. Ways of synchronizing data should be developed in personal devices with a back-up server effortlessly serving the user, securely and without wires.

3.2 Socio-economic safeguards

Standards

Open standards

Open systems are considered by many experts as the only way to achieve two important goals: interoperability and competition [30, 4]. Interoperability means that independently developed systems or components can connect to each other, exchange information and operate in tandem without loss of functionality. Because of the complexity and diversity of the components that make up an AmI network, interoperability is one of its biggest technical challenges. The research and business community will take any technique seriously if it can increase interoperability.

Apart from the positive effects of open innovations as such, the development of protection software (against viruses, spam, spyware, etc.) should be supported under the open source development model and made available to every citizen free of charge. Though open source is no panacea for security problems, there is evidence that open source software can lead to robust and reliable products. But, as Hansen et al. (2002) state, "No single state can finance this development alone" [13, 23].

ISO standards

Among the ISO (International Organization for Standardization) standards relevant to privacy, identity and, in particular, information security is ISO/IEC 15408 on evaluation criteria for IT security and ISO 17799, the Code of practice for information security management. The ISO has also established a Privacy Technology Study Group (PTSG) under Joint Technical Committee 1 (JTC1) to examine the need for developing a privacy technology standard.

From access control to public private partnerships

We can assume that, for the most part, AmI networks will be installed by the private sector and, consequently, they will be seeking to recover their costs and make a profit from their subscribers and/or those willing to pay for a service on an ad-hoc basis. Hence, some form of access control, linked to individual identifiers and/or attributes, will be important to cost recovery. One could speculate that the private

sector will want to form public private partnerships (PPPs) to minimise their costs in deployment of AmI networks, and that a part of that PPP initiative will involve agreement on appropriate access control measures. If that is the case, it will provide an important impetus towards standardisation of identity and access management.

Codes of practice

Various codes of practice for protecting privacy exist. Among the best are those of the OECD, which has been working on privacy issues for many years. Its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, produced more than 25 years ago, are still relevant today and undoubtedly will be relevant in an AmI world. The OECD's more recent (2002) Guidelines for the Security of Information Systems and Networks are also an important reference. In November 2003, the OECD published a 392-page volume entitled Privacy Online: OECD Guidance on Policy and Practice, which contains specific policy and practical guidance to assist governments, businesses and individuals in promoting privacy protection online at national and international levels.

Service contracts

A possible safeguard is a contract between the service provider and the user that has provisions about privacy rights and the protection of personal data and notification of the user of any processing or transfer of such data to third parties. While this is a possible safeguard, there must be some serious doubt about the negotiating position of most individual users. Also, from the service provider's point of view, it's unlikely that he would want to conclude separate contracts with every single user.

Trust marks and trust seals

Trust marks and trust seals can also be useful safeguards because the creation of public trust is a good way for organisations to alert consumers and other individuals to the organisation's practices and procedures through participation in a program that has an easy-to-recognise symbol or seal. Trust marks and seals are a form of guarantee provided by an independent organisation that maintains a list of trustworthy companies that have been audited and certified for compliance with some industry-wide accepted or standardised best practice in collecting personal or sensitive data. Once these conditions are met, they are allowed to display a trust seal logo or label that customers can easily recognise [24, 32].

Trust seals and trust marks are, however, voluntary efforts that are not legally binding and an effective enforcement needs carefully designed procedures and the backing of an independent and powerful organisation that has the confidence of all affected parties.

Examples of such trust marks are those of TRUSTe[5], BBBOnline[6], CPA WebTrust[7], OPA (Online Privacy Alliance) , and VeriSign[8].

Privacy audits and certificates

Audit logs may not protect privacy since they are aimed at determining whether a security breach occurred (i.e., after the fact) and, if so, who might have been responsible or, at least, what went wrong, but they may have a deterrent value. The ISO 17799 (see above) standard contains provisions for audit logs. In the highly networked environment of our AmI future, maintaining audit logs will be a much bigger task than now where discrete systems can be audited. Nevertheless, those designing AmI networks should (be required to) ensure that the networks have features that enable effective audits.

Education

A self-aware, critical and responsible approach to ICTs is the best protection against many risks that could arise in an ambient intelligence society. In terms of general education, this means that the priorities should not be the pointless learning of skills for dealing with ICTs, but the acquisition of meaningful knowledge and a critical basic attitude.

Public awareness and acceptance

Perhaps one of the best safeguards against intrusions of our privacy is public opinion, stoked by stories in the press and the consequent bad publicity given to perceived invasions of privacy by industry, government and other miscreants. Media attention follows its own logic, however, which makes publicity more or less erratic and difficult to rely on.

A recent survey found that less than one in ten IT directors could actually define an identity management system [33]. If IT directors have such a low awareness of identity management, then public awareness will be an order of magnitude less. Nevertheless, the media attention given to identity theft and breaches of personal data held by numerous companies is surely helpful in raising public awareness, in drawing to the public's attention that there is a problem here.

[5] The TRUSTe program (http://www.truste.org) was released in 1997 by a consortium of CommerceNet, the Electronic Frontier Foundation (EFF) and the Boston Consulting Group as an independent, non-profit organisation.

[6] BBBOnline (http://www.bbbonline.org) was released in 1999, by the Better Business Bureau (BBB). BBB is an independent US business service "dedicated to fostering fair and honest relationships between businesses and consumers, instilling consumer confidence and contributing to an ethical business environment".

[7] CPA WebTrust (http://www.cpawebtrust.org) was released in 1997 by the American Institute of Certified Public Accountants.

[8] VeriSign (http://www.verisign.com).

An alternative strategy to actively improve awareness and acceptance are roundtables. Holding roundtables at public research institutions and possibly even at industry research laboratories can help to involve society in the research process, avoid misunderstandings and alleviate reservations. These events should be used to steer developments in a desirable direction by identifying possible conflicts at an early stage and to solve them before they become momentous.

3.3 Legal and Regulatory Safeguards

There exist well-established privacy and data protection laws in Europe, aimed at protecting the privacy of the individual. The most relevant European legislation is certainly provided in the data protection directive 95/46/EC and the privacy and electronic communications directive 2002/58/EC. While trying to solve the problems which might occur in AmI, as foreseen by the SWAMI dark scenarios, using the existing legal framework, one is likely to encounter other problems, for which the current laws and regulations do not provide a solution. Thus, the legal and regulatory framework will need to develop further in order to take into account the new AmI world.[9]

It needs to be emphasised, however, that simply having legislation, such as Europe's data protection directive, is obviously useless unless the legislation has teeth, i.e., that it can be enforced.

Accessibility and inclusion

At a very general level, law-making within the EU should keep up its efforts in putting special emphasis on equality of rights issues in order to ensure that all citizens have the chance to benefit from the new opportunities AmI technologies will offer. Policies should generally strive to remove direct and indirect discrimination, for instance, by fostering broad and affordable access to services and by implementing targeted actions (training, education, etc.) in favour of under-represented user groups. Also, for the sake of sustained acceptance of AmI, regulatory policies should aim to strike a fair balance between legitimate but nonetheless partially conflicting interests of industry, consumers and citizens.

Accountability, audits, international collaboration and enforcement

Service providers who provide identity management services and/or those who hold personally identifiable information (such as supposed Trusted Third Parties) should be held accountable for compliance with legislation and regulation governing their services and subject to regular independent audits.

[9] A much fuller discussion of legal and regulatory safeguards will appear in the next SWAMI D3 deliverable.

Actions by the European Commission and the Member States

Currently, any proposals made to the European Commission under its Framework Programmes must explicitly conform to certain ethical rules, EU legislation and international conventions, and indicate how they intend to "integrate" the gender dimension. Commission guidelines specifically say that proposals must conform to, inter alia, the data protection directive 95/46/EC, but one can assume that most proposals interpret this conformity requirement in a narrow sense (i.e., that the proposal partners will not be compiling a database with personal data, nor processing and transferring such data to a non-EU country without the subjects' consent). Such a provision is useful as far as it goes, of course, but the Commission should go beyond this by requiring those making proposals to indicate whether or how any new technology developed with EC funding might have privacy impacts.

Guidelines for ICT research

Government support for new technologies should be linked more closely to an assessment of technological consequences. On the basis of the far-reaching social effects that ambient intelligence is supposed to have and the high dynamics of the development, there is a clear deficit in this area [20]. Research and development (at least publicly supported R&D) must highlight future opportunities and possible risks to society and introduce them into public discourse. Every research project should commit itself to explore possible risks in terms of privacy, security and trust, develop a strategy to cover problematic issues and involve users in this process as early as possible.

Public procurement

If the state acts as a buyer of strategically important innovative products and services, it is able to create the critical demand that enables suppliers to reduce their business risk and realise spillover effects. Thus, public procurement programs can be used to support the demand for and use of improved products and services in terms of security and privacy or identity protection.

In the procurement of ICT products, emphasis should therefore be given to critical issues like security and trustworthiness. As in other advanced fields, it will be a major challenge to develop a sustainable procurement policy that can cope with ever-decreasing innovation cycles. The focus should not be on the characteristics of an individual product or component, but on the systems into which components are integrated.

References

[1] Ahmed, A. A. E. and Traore, I. (2005). Anomaly intrusion detection based on biometrics. In *Proceedings of the 2005 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY June 2005*.

[2] Ailisto, H., Lindholm, M., Mantyjarvi, J., Vildjiounaite, E., and Makela, S.-M. (2005). Identifying people from gait pattern with accelerometers. In Carapezza, E. M., editor, *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IV*, volume 5779 of *Proceedings of the SPIE*, pages 7–14.

[3] Ailisto, H., Vildjiounaite, E., Lindholm, M., Mäkelä, S.-M., and Peltola, J. (2006). Soft biometrics — Combining body weight and fat measurements with fingerprint biometrics. *Pattern Recognition Letters*, 27:325–334.

[4] Alvestrand, H. (2004). The role of the standards process in shaping the Internet. *Proceedings of the IEEE*, 92(9):1371–1374.

[5] Blarkom, G. W. v., Borking, J. J., and Olk, J. G. E., editors (2003). *Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents*. TNO-FEL, The Hague.

[6] Camenisch, J. (2005). First annual research report. PRIME Deliverable D16.1. http://www.prime-project.eu.org/public/prime_products/deliverables/rsch/pub_del_D16.1.a_ec_wp16.1_V1_final.pdf.

[7] European Commission (2002). *e*Europe 2005: An information society for all. An Action Plan to be presented in view of the Sevilla European Council, 21/22 June 2002. COM (2002) 263 final, Brussels.

[8] European Commission (2003). *IST 2003 — The Opportunities Ahead*. Office for Official Publications of the European Communities, Luxembourg.

[9] European Commission (2005). i2010 — A European Information Society for growth and employment. COM (2005) 229 final, Brussels.

[10] Giddens, A. (1990). *The consequences of modernity*. Polity Press, Cambridge.

[11] Grabner-Kräuter, S. and Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies*, 58(6):783–812.

[12] Hansen, M., Krasemann, H., Borking, J., Camenisch, J., Sommer, D., Fischer-Hübner, S., Andersson, C., Lacoste, G., Leenes, R., Mitchison, N., Sanna, A., Tseng, J., Pau, L.-F., and Willigens, J.-M. (2005). Privacy and identity management for Europe — White paper. PRIME Deliverable D 15.1.d. http://www.prime-project.eu.org/public/prime_products/deliverables/WPaper/pub_del_D15.1.d_ec_wp15.1_final.pdf.

[13] Hansen, M., Köhntopp, K., and Pfitzmann, A. (2002). The open source approach — Opportunities and limitations with respect to security and privacy. *Computers and Security*, 21(5):461–471.

[14] HiSPEC (2002). Privacy enhancing technologies: State of the art review, version 1. HiSPEC report. http://www.hispec.org.uk/public_documents/7_1PETreview3.pdf.

[15] Hoffmann, M., Wang, H., Eisenhauer, M., Heikkinen, S., Kontopoulou, S., and Xenakis, C. (2006). Security & trust: Cross layer issues. Technical report, Wireless World Research Forum, Special Interest Group 2 "Security and Trust".

[16] Ihde, D. (1996). *Technology and the Lifeworld: From Garden to Earth*. Indiana University Press, Bloomington, Ind.

[17] ISO/IEC (2005). Information technology — Security techniques — Code of practice for information security management. ISO/IEC 17799:2005(E), International Standardisation Organisation.

[18] IST Advisory Group (2002). *Trust, dependability, security and privacy for IST in FP6*. Office for Official Publications of the European Communities, Luxembourg.

[19] Kent, S. T. and Millett, L. I., editors (2003). *Who Goes There?: Authentication Through the Lens of Privacy*. National Academies Press, Washington, DC.

[20] Langheinrich, M. (2003). The DC-privacy troubadour — Assessing privacy implications of DC-projects. In *Designing for Privacy Workshop. DC Tales Conference*, Santorini, Greece.

[21] Luhmann, N. (2000). *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*. Lucius & Lucius, Stuttgart, 4th edition.

[22] Nixon, M., Carter, J., Shutler, J., and Grant, M. (2002). New advances in automatic gait recognition. *Elsevier Information Security Technical Report*, 7(4):23–35.

[23] Payne, C. (2002). On the security of open source software. *Information Systems Journal*, 12(1):61–78.

[24] Pennington, R., Wilcox, H. D., and Grover, V. (2004). The role of system trust in business-to-consumer transactions. *Journal of Management Information System*, 20(3):197–226.

[25] Popitz, H. (1968). *Über die Präventivwirkung des Nichtwissens: Dunkelziffer, Norm und Strafe*, volume 350 of *Recht und Staat in Geschichte und Gegenwart*. J. C. B. Mohr, Tübingen.

[26] 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., and Vildjiounaite, E. (2005). Safeguards in a world of ambient intelligence (SWAMI): Dark scenarios on ambient intelligence — Higlighting risks and vulnerabilities. SWAMI Deliverable 2. http://swami.jrc.es

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

[28] Schneier, B. (2003). The future of surveillance. *Crypto-Gram Newsletter*, 15 October 2003. http://www.schneier.com/crypto-gram-0310.html

[29] Schreurs, W., Hildebrandt, M., Gasson, M., and Warwick, K. (2005). Report on actual and possible profiling techniques in the field of ambient intelligence. FIDIS Deliverable D7.3. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.3.ami_profiling.pdf

[30] Simon, K. D. (2005). The value of open standards and open-source software in government environments. *IBM Systems Journal*, 44(2):227–238.

[31] Spiekermann, S. and Pallas, F. (2006). Technology paternalism – wider implications of ubiquitous computing. *Poiesis & Praxis*, 4(1):6–18.

[32] Subirana, B. and Bain, M. (2005). *Legal Programming: Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond*. Integrated Series in Information Systems. Springer, New York.

[33] Thomson, I. (2005). Government regulation driving ID management. *vnunet.com*. 26 Apr 2005. http://www.vnunet.com/vnunet/news/2127216/government-regulation-driving-id-management.

Part II

Abstracts of presentations

Wiring in Humans

Advantages and problems as humans become part of the machine network via implants

Kevin Warwick*

University of Reading, Department of Cybernetics, Whiteknights, Reading, RG6 6AY, United Kingdom, kw@cyber.rdg.ac.uk

In this presentation a look will be taken at how the use of implant technology is rapidly diminishing the distance between humans and intelligent networks. In effect as a human is wired in to the network they become a part of that ambience themselves. This can have a tremendous impact in the treatment of different neural illnesses. An indication will be given of a number of areas in which such technology has already had a profound effect, a key element being the need for a clear interface linking the human brain directly with a computer. However, in order to assess the possible opportunities, both human and animal studies from around the world will be reported on.

The main thrust will be an overview of Kevin's own research which has led to him receiving a neural implant which linked his nervous system bi-directionally with the internet. With this in place neural signals were transmitted to various technological devices to directly control them, in some cases via the internet, and feedback to the brain was obtained from such as the fingertips of a robot hand, ultrasonic (extra) sensory input and neural signals directly from another human's nervous system.

* Dr Kevin Warwick is Professor of Cybernetics at the University of Reading, where he carries out research in artificial intelligence, control, robotics and biomedical engineering. He held positions at Oxford, Newcastle and Warwick Universities before being offered the Chair at Reading at the age of 33. He has been awarded higher doctorates both by Imperial College and the Czech Academy of Sciences, Prague and has been described as Britain's leading prophet of the robot age. Kevin carried out a series of pioneering experiments involving the neuro-surgical implantation of a device into the median nerves of his left arm in order to link his nervous system directly to a computer to assess the latest technology for use with the disabled. He was successful with the first extra-sensory (ultrasonic) input for a human and with the first purely electronic communication experiment between the nervous systems of two humans. His research has been discussed by the US White House Presidential Council on BioEthics, The European Commission Group on Ethics in S & T and has led to him being widely referenced and featured in academic circles as well as appearing as cover stories in several magazines – e.g. Wired (USA), The Week (India), Mensa (UK), I-Magazine (Germany), L'Espresso (Spain). Further information can be found at: www.kevinwarwick.com

A view will be taken as to the prospects for the future, both in the near term as a therapeutic device and in the long term as a form of enhancement, including the realistic potential, in the near future, for thought communication – thereby opening up tremendous commercial potential. Clearly though, an individual whose brain is part human - part machine can have abilities that far surpass those who remain with a human brain alone. Will such an individual exhibit different moral and ethical values to those of a human? If so, what effects might this have on society?

Mr. Rocky Bottoms Encounters 35 Techno-Fallacies

A Fictional Speech and Critical Analysis

Gary T. Marx*

6209 E. Kelton Lane, Scottsdale, AZ 85254, U.S.A, gtmarx@garymarx.net

In generating light upon the goal of creating light rather than the dark side futures so creatively imagined by the SWAMI project, I offer a speech by a fictional character –police officer, engineer, intelligence agent and now security consultant Mr. Rocky Bottoms to the American-Euro Society for Surveillance. Bottoms' speech is a composite of actual arguments put forth by business and government leaders who have an unquestioned optimistic oversimplified faith in science and technology as solutions to social issues. Such leaders argue for unleashing the technology and the maximization of economic and security values above everything else In response, I note some conceptual distinctions and identify 35 "techno-fallacies" commonly heard in such advocacy. The fallacies may be empirical, logical or at the level of values. Along with positive policies, laws and technical developments, we need to continually interrogate our culture and identify and ask critical questions about the invisible assumptions that accompany the creation and implementation of AmI and related information environments.

* Gary T. Marx is Professor Emeritus M.I.T. He received his PhD from the University of California at Berkeley where he began his teaching career. He has taught and lectured in a number of countries. His work has appeared in over 300 books and periodicals and is translated into many languages. He is the author of Undercover: Police Surveillance in America and of the forthcoming Windows Into the Soul: Surveillance and Society in an Age of High Technology. Additional information is at wwwgarymarx.net.

Combating Criminality in a World of Ambient Intelligence

Gus Hosein*

London School of Economics and Political Science, Department of Information Systems, Houghton Street, London WC2A 2AE, United Kingdom, i.hosein@lse.ac.uk

In this talk I will review the legal and regulatory structures that we have been building to deal with the 'new technological environment' in our midst. In particular I will review some of the more complex surveillance policy debates. The technology-neutral approach to policy can lead to some very interesting scenarios in the world of ambient intelligence. I will draw from our experiences in moving from a world of telephony to digital telephony to understand the new challenges that we will likely encounter.

* Gus Hosein is a Visiting Fellow in the Department of Information Systems at the London School of Economics and Political Science. He is also a Senior Fellow with Privacy International, and an advisor to a number of non-governmental, governmental, and inter-governmental organisations. For more information please see http://personal.lse.ac.uk/hosein

AmI – The European Perspective on Data Protection Legislation and Privacy Policies

Martin Meints* and Henry Krasemann

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Postfach 71 16, D-24171 Kiel, Germany, LD102@datenschutzzentrum.de

This talk introduces the legal grounds of data protection for AmI. In the second part the suggestions of the Art. 29 Working Party with respect to privacy policies are introduced and current research to implement privacy policies is summarised. The third part presents open aspects in legislation and implementation of law, limitations we can observe today and future trends for AmI.

* Dr. Martin Meints studied chemistry and computer science at the University Kiel. He worked in various enterprises and public organisations as IT project manager and in technical management functions. Main focus of his latest work was preparation and implementation of security concepts for large private networks (LAN and WAN) and integrated mobile computing solutions basing on the methodology of the Baseline Protection Manual from BSI, the German Federal Office for Information Security. Since 2004 researcher for the Independent Centre for Privacy Protection Schleswig-Holstein (ICPP); he is mainly involved in the project "FIDIS – Future of Identity in the Information Society".

Privacy in pervasive computing environments – A contradiction in terms?

Johann Cas*

Austrian Academy of Sciences, Institute for Technology Assessment, Strohgasse 45, A-1030 Vienna, Austria, jcas@oeaw.ac.at

Within the next future, continuing technical progress in electronics will allow to transform current visions of pervasive computing into real world options. This perspective has raised deep concerns about the survival of privacy as central building blocks of pervasive computing are in direct conflict to the fundaments of privacy protection. Considerable efforts have been undertaken to cope these concerns with, however, only limited success. While pertinent efforts resulted in solutions for single aspects they proved insufficient to eliminate the fears; on the contrary, they highlighted the principal incompatibility of privacy and pervasive information systems. Technical concepts alone, regardless how complex they are, cannot be sufficient; rather, a mix of privacy enhancing technologies, restrictions on the utilization of pervasive computing, and new regulations will be required to preserve some remnants of privacy.

* Johann Cas, born 1957. Higher Technical Teaching College, Klagenfurt, Department of Telecommunications; 1987: degree in economics at the University of Graz; technical consultant in industrial automation; since 1988 employed by the ITA as specialist in information society technologies; main focus at present: privacy in the information society, privacy enhancing security technologies.

Building Privacy-aware AmI Systems

Marc Langheinrich*

ETH Zurich, Inst. for Pervasive Computing, Clausiusstr. 59, 8092 Zurich, Switzerland,
langhein@inf.ethz.ch

The Fair Information Practices with their principles of Notice and Choice are the cornerstone of many privacy laws worldwide. As such, it is only natural that one should try to include these principles in AmI-Systems in order to make them privacy friendly. However, both consumer surveys and actual consumer behavior often show that people are willing to trade large parts of their personal information for tangible benefits like convenience, lower prices, and security/safety. Given the rise of data collections in AmI, is it still apropriate to burden the user with such decisions.

* Marc is a lecturer at the Institute for Pervasive Computing at the ETH Zurich, Switzerland. He holds a Master's in Computer Science (Dipl.-Inf.) degree from the University of Bielefeld, Germany, and received a PhD from the ETH Zurich for his work on privacy in ubiquitous computing. Marc is one of the authors of P3P, a W3C-standard for machine-readable privacy policies on the Web.

Privacy Incorporated Software Agents

Jan Huizenga*

TNO Information and Communication Technology, P.O.Box 5050, Roeselaerestraat 43, 2600 GB Delft, The Netherlands, J.Huizenga@telecom.tno.nl

Intelligent Software Agents (ISA) & Privacy: One of the objectives of the PISA consortium was to support the design and evaluation of Information and Communication Technology so that the informational privacy of the user is protected. We present the case how to incorporate privacy-protecting features into an ISA. The PISA consortium has developed a new privacy threat analysis, a new cryptographic algorithm and privacy ontologies, but also the architecture of PISA is innovative and harbours legal knowledge, as well new applications of privacy enhancing technologies (PET). Further research will be point out to tackle new cryptographic solutions for untrusted mobile platforms. Also new ambient technologies as RFID tags for identification and tracking and tracing of objects and persons are studied now to advice about privacy implications and technical and organisational privacy protecting solutions.

* Jan Huizenga is Business Consultant within TNO Information and Communication Technology, focussing on the public sector and the security industry in ICT. He received his M.Sc. degree in Electrical Engineering from the Delft University of Technology (Delft, The Netherlands). He is involved in research for security-studies and development of new techniques for mobile commerce and security/privacy. He was the project co-ordinator for the EC PISA-project (Privacy Incorporated Software Agent, IST 2000-26038). The work in PISA has also been continued together with TUD, UTwente and KUN in the "Privacy in an Ambient World" (PAW: www.cs.ru.nl/paw/) project, supported by the Dutch government in the Ministry of Economical Affairs "GenCom" program.

Enhancing trust by implementing Identity Assurance

Maarten Botterman*

RAND Europe, Meerum Terwogtlaan 269, 3056 PP Rotterdam, The Netherlands,
maarten@rand.org

In today's society, in which more and more business is done online, Identity is fast becoming the 'single organising principle' around which businesses, governments and the citizen interact. Despite recent political attention and media hype about identity cards, identity theft, on-line fraud and privacy concerns, the debate about the way ahead on "Identity Assurance" (IdA) is yet to begin. IdA is defined as: a framework of technical, management, policy and regulatory initiatives aimed at preserving the confidentiality, integrity and privacy of identity related data, as well as the availability of information infrastructures and supporting identity management systems.

The development of this framework is not an easy task. Identities are formed by collating data on a person, business, animal or object. Whereas this was a cumbersome process when identities were purely paper based, the advantages of digital collection, storage and retrieval of personal data come at a cost: it is now possible to collect so much information so quickly from a large set of sources on persons (allowing, for instance, profiling). Identity is also central in securing data. Identity Management Systems (IDM) are crucial for user account management for the authentication and authorising of system users. An identity assurance framework must embody the interests and objectives of all stakeholders who operate and benefit from them: industry (developers and users), government (users and service providers) and

* Maarten Botterman is Director of Information Society Policy Research at RAND Europe and as such responsible for initiating, managing, quality assurance and knowledge (team) building activities focused at the information society aspect of policy. He is also CEO of the UK based Information Assurance Advisory Council (www.iaac.org.uk). He holds a masters degree in business economics from Erasmus University Rotterdam. Maarten has been working on issues relating to information security, implementation of ICTs in ways to work, and governance in the Information Society since 1987. Before his assignment at RAND Europe he was Scientific Officer within the European Commission, DG Information Society. Before that he worked at the Dutch Ministry of Transport, Public Works and Water Management, initially as Head of an Information Management and EDP department, later as Senior Telework Consultant and Senior Policy Advisor on Transport Telematics. Per May 1st 2006 he will leave RAND and set up his business as independent consultant on information society impact, information assurance,and corporate social responsibility.

civil society. It must take into account the issue of controls. Who controls the use of my identity, who controls the mechanisms for exceptional use, who controls the custodian of the personal datasets that make up my identity, etc. The framework must be outward looking, taking into consideration the international context, and learn from practice elsewhere. As in the case of information assurance, identity assurance seeks to enhance online security and trust.

Building up to that framework some key points converge from the initial survey and debates in the UK. These results will be presented to the SWAMI forum.

Security concerns as viewed by the Wireless World Research Forum

Mario Hoffmann*

Fraunhofer Institute for Secure Information Technology SIT, Rheinstrasse 75, 64295 Darmstadt, Germany, Mario.Hoffmann@sit.fraunhofer.de

"7 trillion wireless devices serving 7 billion people in 2017", Wireless World Research Forum - WWRF

The WWRF is a global organisation, which was founded in August 2001. The objective of the forum is to formulate visions on strategic future research directions in the wireless field, among industry and academia, and to generate, identify, and promote research areas and technical trends for mobile and wireless system technologies.

The presentation will introduce the mission of and most related work achieved within the special interest group "Security and Trust - SIG2" of the Wireless World Research Forum (WWRF) founded in 2003.

SIG2 is focussed on identifying and promoting research areas that strive to understand and resolve the needs of users, operators, service providers and other players for secure and trustworthy wireless systems. Resolving these issues is a necessary part of WWRF's mission to guide the research and development of applications, services and underlying technologies. The SIG will gather inputs and views from both industry and academia, synthesize these views to influence future visions and research priorities and share results across the forum.

For details see: http://www.wireless-world-research.org/

* Mario D. Hoffmann was born in Neuwied am Rhein, Germany, 1970. In 1999 he received his master degree in computer science from Darmstadt University of Technology, Darmstadt, Germany. Since 2004 he has been leading the research department for Secure Mobile Systems at Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt, Germany. His current research interest in his PhD thesis is dedicated to multilateral secure identity management for context-aware mobile services.

Anonymity, unobservability, pseudonymity and identity management requirements for an AmI world

Andreas Pfitzmann*

Dresden University of Technology, Department of Computer Science, Institute for System Architecture, 01062 Dresden, Germany, pfitza@inf.tu-dresden.de

Ambient Intelligence may be at odds with central values of the European Constitution – at least as long as security of ICT in general and of open ICT infrastructures in particular is only roughly as bad as today. Security breaches are particularly severe w.r.t. privacy, since damage cannot be compensated for later on – if you have lost a secret, it is lost.

Therefore, mechanisms to provide for anonymity or even unobservability in using networks and services have been developed to limit breaches of privacy. Pseudonymity can be used to provide for suitable compromises between the individuals wish for privacy and the equally legitimate wish of communication and business partners for authenticity and accountability. Privacy-enhancing identity management (PE-IDM) provides the framework to make good use of pseudonymity. Therefore, I discuss whether and under which conditions PE-IDM can be used in an AmI world.

* Andreas Pfitzmann is a professor of computer science at Dresden University of Technology. His research interests include privacy and multilateral security, mainly in communication networks, mobile computing, and distributed applications. He is a member of ACM, IEEE, and GI, where he served as chairman of the Special Interest Group on Dependable IT-Systems for ten years.

Empowerment and Context Security as the route to Growth and Security

Stephan Engberg*

PRIWAY, Stengaards Alle 33D, 2800 Kgs. Lyngby, Denmark,
Stephan.Engberg@priway.com

The old security paradigm focussing on Central Command & Control and pervasive Surveillance is creating more and more risks without creating trust or value. Despite subjective and often even appearing not rational, consumer risk perception is slowly aligning with reality driving distrust and growing resistance. Identity Theft are in the process of alligning Security & Privacy while teaching us that Identification of people and devices are destructive for Trust & Security.

In the middle of a political climate turned paranoid and outdated security myths related to biometrics, identification and surveillance, we face the need to change to meet the ambient challenges. We know how - empower the users for demand-pull and

* Stephan J. Engberg is specialised in Trust Socio/Economics. Since 1999 he has been focused on Identity Management, Privacy Enhancing Technologies and increasingly Identity Theft, in order to design security into technology, services and products to overcome the growing distrust and security problems. He is a serial entrepreneur, lately as founder of Priway (www.priway.com) and the spin-off RFIDSec (www.rfidsec.com). — RFIDsec is providing RFIDs with built-in context management based on low-computational Privacy Enhancing protocols. Priway is providing user-centric Identity Management focussing on Citizen ID Cards and making "trusted" parties trustworthy by enabling channel management for identity management. — Stephan Engberg has been working with security roadmapping and research in connection with the EU IST Framework programme 6 (Roadmap for Advanced Research in Privacy & Identity management) and as member of the SecurIST Advisory Board working on FP7 security research roadmapping. In addition he was involved with the EU i2010 programme on security. Priway is partner in a starting IST IP-protect called "HYDRA" on middleware for enabling Embedded Systems to integrate semantically. — Stephan Engberg has been lecturing on consumer loyalty since 1996 and increasingly in a range of security and trust related topics. He is author of multiple papers, articles, books, and are often invited to talk on issues related to security and privacy in the Integrated Networked Economy. He has workedt 9 years in banking, 3 years as an entrepreneur in optical telecommunications and as executive management consultant in CRM and eBusiness strategy. He holds a M.Sc. in Business Administration and Computer Science from Copenhagen Business School combined with studying innovation and international strategy at London Business School.

ensure system dependability through virtualisation. We have outstanding technical and especially usability challenges but the important barriers are mental.

Using RFID to illustrate how RFID with PETs entering the market address problems and solve a long range of Trust, Security & Privacy issues - the question of a market-driven road to privacy driving Growth & Security with respect for European values are discussed.

Security requirements in the context of AmI systems

Reinhard Schwarz*

Fraunhofer Institute Experimental Software Engineering IESE, Fraunhofer-Platz 1, 67663 Kaiserslautern, Germany, reinhard.schwarz@iese.fraunhofer.de

Providing adequate and predictable security is a challenge even for conventional IT systems. The AmI paradigm exacerbates the problem. While some technical solutions for selected AmI component security problems have been suggested, we still lack »the big picture« how to tackle security at system level. Putting aside technical details, some of the most critical issues in determining and enforcing AmI security requirements are:

1. Dynamic AmI configurations are a moving target for static security analysis.
2. AmI security has a number of conflicting goals that are hard to reconcile.
3. Ubiquity and openness make it very hard to confine confidential information to the intended usage.

Having specified a set of security requirements, an open problem is how to validate these requirements for completeness, correctness and consistency, and how to enforce them in subsequent development lifecycle phases, particularly under AmI resource constraints.

* Dr. Reinhard Schwarz studied computer science and received his Ph.D. from Kaiserslautern University of Technology. He is heading the Security and Safety department at the Fraunhofer Institute for Experimental Software Engineering, Kaiserslautern. His reseach interests include secure software engineering, security in the context of embedded and ambient systems, and tools for security evaluation.

Regulating Ambient Intelligence
The Road to Privacy Impact Assessment?

Charles D. Raab*

University of Edinburgh, School of Social and Political Studies. Adam Ferguson Building, George Square, Edinburgh EH8 9LL, Scotland, United Kingdom, c.d.raab@ed.ac.uk

SWAMI's scenarios and analyses examine the impact of AmI on a host of personal, social, and other values, including privacy, security, identity, exclusion, etc. They aim to understand how risks on the 'dark' side of these technological developments can be minimised. It is important to build upon this work by considering regulatory roles and strategies deployable in AmI contexts by individuals, organisations, states and technologists. One implication of SWAMI is that impact assessments for privacy and other values might be an important adjunct of these regulatory efforts. This short presentation will address these topics.

* Charles D. Raab is Professor of Government in the University of Edinburgh, and has published extensively on information policy, especially concerning privacy protection. He is co-author (with Colin Bennett) of The Governance of Privacy: Policy Instruments in Global Perspective (2003; 2nd edition 2006), and (with Malcolm Anderson et al.), of Policing the European Union (1995). He co-authored (with Colin Bennett et al.,) a report for the European Commission (1999) on the adequacy of data protection in non-EU countries, and (with Perri 6 et al.) a report for the Scottish Executive (2004) on information sharing and privacy with regard to child protection. He has investigated the implications of GIS for privacy, identity and boundaries; identity management (the 'PRIME' project); and data-sharing and privacy in multi-agency working in the UK. He served on the Advisory Board for the Cabinet Office report, Privacy and Data-Sharing: The Way Forward for Public Services (2002). He is an Associate of the AHRC Research Centre for Studies in Intellectual Property and Technology Law at the University of Edinburgh, and a member of the Data Protection Research and Policy Group of the British Institute of International and Comparative Law. He serves on the editorial boards of six academic journals in this field of study.

Security concerns associated with digital territories

Achilles Kameas*

Hellenic Open University, 23 Sahtouri str, 26222 Patras, Greece,
kameas@math.upatras.gr

The term "digital territory" (DT) has been coined in an attempt to port a real world metaphor into the forthcoming synthetic world. This new term carries certain assumptions and gives rise to sub-concepts; it requires a certain level of technology and will be realised at a pace affected by specific factors; once adopted, it shall cause an imbalance to existing personal and social structures. A DT is an ephemeral AmI space: it is created for a specific purpose and integrates the will of the owner (an individual or group operator) with the means to achieve it (including infrastructure, properties, services and objects) within an AmI space.

In such an environment which is extremely personalised, the protection of personal data which are networked and therefore remotely accessible is very important. The natural way to achieve this is by establishing boundaries – digital boundaries which people tend to accept intuitively. Boundaries need to be well-defined points in the digital environment. They should be easily perceivable by all individuals active in the digital context. In order for them to operate properly, boundaries in the digital environment must become as clear as boundaries in the real world.

Security and privacy concerns are associated with all categories of DTs, such as location based systems and services, virtual residencies and mobile phone networks. DTs and their components including the whole infrastructure they rely on are exhibited to security, privacy, identity and copyright related threats. These threats range from unauthorized information manipulation and disclosure (violations of personal or corporate confidentiality), to forgery, denial of service, profiling, and piracy or cloning. To cope with, suitable measures have to be taken which include organiza-

* Achilles D. Kameas received his Engineering Diploma (1989) and his Ph.D. (1995, in Human-Computer Interaction), both from the Department of Computer Engineering and Informatics, Univ. of Patras, Hellas. Since 2003, he is an Assistant Professor with the Hellenic Open University, where he teaches software design and engineering. He is also R&D manager with Research Academic Computer Technology Institute (CTI), where he is the head of Research Unit 3 (Applied Information Systems) and the founder of DAISy group (http://daisy.cti.gr). He served as an elected member of the Disappearing Computer steering group; currently he is a member of the Convivio network steering group. In 2005, he was the scientific coordinator of the "Study on Digital Territories" funded by JRC/IPTS.

tional, procedural and technical measures, such as entity and data authentication, data and traffic data confidentiality, authorization and access control, digital signatures, privacy and copyright protection.

Discovery, expression and responsibility

Design dimensions for ambient intelligence

Jeffrey Burke*

University of California at Los Angeles, HyperMedia Studio, 102 East Melnitz Hall, Los Angeles, CA 90095, U.S.A, jburke@ucla.edu

Networked sensing enters the public sphere in personal, social and urban contexts. It overlays most parts and places of our lives, including those that are not (and never were) purely work or play. Efficiency is a typical design goal for technology in both productivity and leisure applications: optimizing either task completion or entertainment per unit time. Privacy could be seen to trump all other concerns over data in both domains. But there is a third class of application, where all bets are off with respect to our time. In them, efficiency is neither the right metric nor a primary design goal and sharing of information may weigh equally with privacy. Civic engagement, creative expression, family and community life, the cultural contribution of art, science and engineering: these are for what and for whom we maximize our time. They relate deeply to our physical context and our responsibilities. Can pervasive urban sensing and mobile technology positively impact quality of life unless they are also explicitly designed for this third thing? What are the design dimensions for systems that support our passions, responsibilities and communities?

* Jeffrey Burke has designed, managed or produced performances, new genre art installations, and new facility construction in eight countries from 1999-2006. In each project, he integrates emerging technologies into systems that support creative and expressive goals. He is Executive Director of REMAP, the Center for Research in Engineering, Media and Performance at the University of California, Los Angeles (UCLA), which is developing a new focus on design methodologies for the use of embedded computing in civic, cultural and social contexts.

Policies for an inclusive European Information Society

Lutz Kubitschke*

empirica Gesellschaft für Kommunikations- und Technologieforschung mbH, Oxfordstr. 2, 53111 Bonn, Germany, Lutz.Kubitschke@empirica.com

This contribution draws upon preliminary outcomes of the eInclusion@EU project funded under the European Union's IST programme. It briefly elaborates on the concept of eInclusion as it has emerged in response to the prevailing digital divide. Further, it provides a systematic overview of eInclusion related policy interventions currently pursued in Europe and beyond. Finally, these policies are discussed in relation to the concept of ambient intelligence.

* Lutz Kubitschke is senior consultant at empirica, an independent research and consultancy organisation based in Bonn, Germany. For almost 10 years now, the focus of his research has been on opportunities and threats of new ICT applications for users with special needs and social at-risk groups. Presently, he is coordinator of the eInclusion@EU project, a 30 months coordination action administered by the eInclusion unit of the European Commission's DG Information Society and Media.

AmI: The Promise, the Price and the Social Disruption

Dimitris Gritzalis*

Athens University of Economics & Business , Department of Informatics, 76 Patission Ave., Athens GR-10434, Greece, dgrit@aueb.gr

The presentation will focus on a brief and comparative review of the security and privacy strategies, which have been or planned to be adopted by three leading international economies, namely: European Union, Japan and the United States, in view of the emerging AmI paradigm. In order to perform this review, the relevant agonies and trends in each national environment, the key players, the rising visions, the national strategic plans, and the research agendas and roadmaps, regarding security, privacy, and the digital divide, will be briefly presented and comment upon, with an eye towards the new treats, vulnerabilities, and risks that have appeared or that are expected to appear in the emerging AmI - UbiComp - UbiNet paradigm.

* Dr. Dimitris Gritzalis is an Associate Professor of ICT Security, at the Dept. of Informatics of Athens University of Economics and Business, where he is leading the Information Security and Critical Infrastructure Protection Research Group. Prof. Gritzalis is a former Associate Data Protection Commissioner of Greece and a former President of the Greek Computer Society. He holds degrees in Mathematics (BSc), Computer Science (MSc) and Critical Information Systems Security (PhD).

Ambient Assisted Living – Preparing a European RTD Programme

Michael Huch*

VDI/VDE Innovation + Technik GmbH, Steinplatz 1, 10623 Berlin, Germany,
Huch@vdivde-it.de

A new European initiative called Ambient Assisted Living is currently prepared by a group a several European states to be implemented during the 7th EU Framework Programme for R&D, based on the Article 169 of the European Treaty (AAL169).

Ambient Assisted Living aims - by the use of ICT products and the provision of remote services including care services – at extending the time older people can live in their preferred home environment by increasing their autonomy, assisting them in carrying out activities of daily living.

Through funding of research and innovation projects, with emphasis on integration of required technologies into relevant products and services, AAL169 aims to reinforce a consolidated European market for AAL products, environments and services.

* Michael Huch studied economics at the University of Heidelberg. Since he joined VDI/VDE-IT in 1998, he has ever worked in projects related to European research and innovation and contributed to studies and evaluations of technology funding programmes. In his current project portfolio, he signs responsible for the two National Contact Points "Innovation" and "Microsystems Technologies" located at VDI/VDE-IT and also disseminates his experience with the European Framework Programme to researchers and policy-makers from the New Member States. Since 2004, he coordinates the project "Ambient Assisted Living" which aims at establishing a new technology funding programme based on article 169 of the European treaty.

Distributing insecurity

Rob van Kranenburg*

Resonance Design, Tentoonstellingslaan 22, 9000 Gent, Belgium, kranenbu@xs4all.nl

The Trust Paradox today states that citizens are not distributing themselves as data into the environment which would open up a new territory of hybrid space for innovation, creative industries and socially and culturally constructive spinoffs of nano and biotech, as they are being reminded 24/7 that the environment is unsafe, unstable and untrustworthy. The result is bottom up online and sensorbased innovation (wikipedia, commons based peer production, thinglink) that will create its own informal networks running parallel to top down systems, such as nation states and the eu itself.

* Rob van Kranenburg (1964) graduated cum laude in Literary Theory at Tilburg University (NL). He went to work with Prof Ronald Soetaert in Ghent, in the Educational Department, developing online learning modules, methods and concepts drawing on the idea of multiliteracies. In 2000 he went to Amsterdam to work as programmer on media education at the centre for culture and politics de Balie and as teacher-coordinator of the new media program in the Film and Television Studies Department at the University of Amsterdam. Feeling it was to young a field to predominantly historize it, he moved to Doors of Perception and co-programmed with John Thackara Doors 7, Flow, the design challenge of pervasive computing. In 2003 he mentored a postgraduate course in performance, theatre and the arts at APT, Arts Performance Theatricality. For the past two years he has been working part time at Virtual Platform, Dutch policy and network organization for e-culture, as interim and now as co-director. As innovation consultant he is mainly involved with negociability strategies of new technologies, predominantly ubicomp and rfid (radio frequency identification), the relationship between the formal and informal in cultural and economic policy, and the requirements for a sustainable cultural economy.

Use of RFID in Ambient Intelligence: critical issues for policy makers

Jay Kishigami*

SSP SI Lab, NTT, 3-9-11, Midoricho, Musashinoshi Tokyo 180-8585, Japan,
jay@ntt.net

The main concept of RFID would be the glue function between Virtual and Real world. This powerful system can give us the fully automatic identification and data capturing. From the communications aspect, this could realize the machine to machine convesation. The critical point is how to link the item ID to the human ID. We, Human being, are milling about day by day from real world to virtual world, as web, database, and email unconsciously. The RFID has the possibility to trace every item with the holder person. This is the problem. To avoid the possible privacy violence, several guideline and policy are issued. PEST (Political, Economical , Social and Technological) approach would be really fit for the RFID application.

* Dr. Junichi (Jay) Kishigami is Vice President and Chief Producer, Convergence, Corporate Management Strategy Division NTT. Dr. Junichi (Jay) Kishigami obtained the degree of Bachelor and Master in Physics at the Hokkaido University in Japan 1980 and obtained his Doctor degree in electronic engineering at the Hokkaido University 1989.From 1994 to 1999 he worked with NTT America as a vice president and general manager at IP HQs in the area of creating and promoting the Internet business both in US and in Japan. His background is variet of field, such as magnetic disk storage, solid state physics, broadband services, ID and metadata analysis, and RFID.

Ambient Intelligence: New ways of innovation for Europe

Emile Aarts*

Philips Research, Building WOp.104, High Tech Campus 36, 5656 AE Eindhoven,
emile.aarts@philips.com

Since the launch of the Ambient Intelligence back in 1999, the vision has developed into a major theme for research in the field of Information and Communication Technology for a wide variety of enterprises throughout Europe. This has led to the general understanding that Ambient Intelligence can be seen as an open initiative to innovation that connect basic research to new business creation.

This lecture addresses the developments and achievements in Ambient Intelligence obtained during the past five years. The emphasis is on four different elements, i.e., science, research and development, business, and dissemination. We also briefly address some of the challenges in the implementation and realization of the vision for the years to come.

* Prof. dr. Emile Aarts holds an MSc. and PhD. degree in physics. For almost twenty years he has been active as a research scientist in computing science. Since 1991 he holds a teaching position at the Eindhoven University of Technology as a part-time professor of computing science. He also serves on numerous scientific and governmental advisory boards. He holds a part-time position of senior consultant with the Center for Quantitative Methods in Eindhoven, The Netherlands. Emile Aarts is the author of five books and more than hundred and forty scientific papers on a diversity of subjects including nuclear physics, VLSI design, combinatorial optimization and neural networks. In 1998 he launched the concept of Ambient Intelligence and in 2001 he founded Philips' HomeLab. His current research interests include embedded systems and interaction technology.

Part III

Conference report

Plenary presentations

David Wright

Trilateral Research & Consulting, 12 Tybenham Road, SW 19 3LA London, United Kingdom, david.wright@trilateralresearch.com

The subject of *Kevin Warwick's* remarks was "Wiring in Humans – advantages and problems as humans become part of the machine network via implants".

In his presentation, Prof Warwick discussed how the use of implant technology is diminishing the distance between humans and intelligent networks. As a human is wired in to the network, he or she becomes a part of the world of ambient intelligence. He described how technology can link the human brain directly with a computer.

Prof Warwick referenced the research which led to his having a surgically implanted neural device linking his nervous system bi-directionally with the Internet. He referenced experiments in which neural signals were transmitted so that they could directly control other various technological devices and how feedback was obtained from the fingertips of a robot hand as ultrasonic (extra) sensory input to another person's nervous system.

He speculated about future directions of his research including the prospects for thought communication and the commercial potential of technologies enhancing the capabilities of the human brain. He touched on the ethical issues involved, partly in response to questions following his presentation.

In his presentation, *Gary Marx* offered a speech by a fictional character – a police officer, engineer, intelligence agent and now security consultant, Mr. Rocky Bottoms – to the American-Euro Society for Surveillance. Bottoms' speech is a composite of actual arguments put forth by business and government leaders "who have an unquestioned, optimistic, over-simplified faith in science and technology as solutions to social issues". Such leaders argue for unleashing technology and maximising economic and security values above everything else. Mr Marx noted some conceptual distinctions and identified 35 "techno-fallacies" commonly heard in such advocacy. The fallacies may be empirical, logical and/or at the level of values. Along with positive policies, laws and technical developments, Mr Marx argued for the need to continually interrogate our culture and to critically question the assumptions that accompany the creation and implementation of AmI and related information environments.

Mr Marx encouraged the SWAMI partners to include cultural safeguards among those that could address the threats and vulnerabilities posed by AmI. He also said

we should always ask why we are implementing particular technologies or why we are implementing those technologies in a particular way. What is the problem we are really trying to address? In response to a question, he noted that DNA as a biometric is not specific just to an individual, but also to a family, so that when we provide DNA, we are exposing the privacy of other members of our family.

Jay Kishigami presented an overview of the use of RFID in Ambient Intelligence and discussed critical issues for policy makers.

RFIDs serve as a kind of glue between the real and virtual worlds. RFID tagging systems provide automatic identification and data capturing, enabling machine-to-machine communications. A critical issue is the linking of a product's identity to a person's identity. RFIDs could be used to link or trace every item to that of an individual, which could create serious privacy problems. To avoid threats to individual privacy, policy and guidelines are appropriate. As RFIDs may have many different ramifications, some beneficial and some that are not, policy and guidelines should be considered from a so-called PEST approach (PEST is the acronym for political, economic, social and technological).

The term "ambient intelligence" was coined by *Emile Aarts* of Philips in 1999. The term and concept was readily adopted by the European Commission and Europe generally. In his presentation, Emile Aarts said that since the launch of the concept of ambient intelligence in 1999, AmI has become a major theme for research in the field of information and communication technology for a wide variety of enterprises throughout Europe. Innovations in ambient intelligence research are expected to generate significant benefits for Europe, not least of which is the generation of new business. He referenced key developments and achievements in ambient intelligence in the past five years and provided a vision of where AmI could lead us in the next 15 or 20 years in several key domains. He said AmI has several characteristics – i.e., embedded, context-aware, personalised, adaptive and anticipatory. He highlighted their application in new display technologies, lighting, electronic papers, tiny cameras, clothes, smart beds, health and medical technologies as well as energy-scavenging technologies.

Session 1 – Privacy in a world of ambient intelligence

Wim Schreurs

Vrije Universiteit Brussel, Faculty of Law, Law Science Technology & Society (LSTS), Pleinlaan 2, 1050 Brussel, Belgium, wim.schreurs@vub.ac.be

The following issues, policies and safeguards were introduced during the several presentations and discussions in the privacy safeguards session.

Information and inclusion in the AmI society

- AmI technology is being developed by industry as an asset. Society is confronted with this technology afterwards and then has to decide what to do with it: society should be included in the process much earlier (as has happened with the 'meeting of minds' consultation of the public on brain-computer interfacing) (S. Gutwirth – G. T. Marx);
- There should be an open, inclusive and informed debate. The problem of influencing and conditioning social expectations of privacy, for example, should be tackled with stories on security;
- There should be a 'multilateral approach' to privacy issues in AmI;
- people should be educated how to use technology (links to digital divide) and this education should be objective, away from industry and governmental interests;
- In addition to privacy threats, secondary risks such as costs and controllability should be highlighted.

Principles of data protection are under attack in AmI, especially those on collection limitation and purpose specification

The threats to data protection principles can be shown, for example, by recent legislation on data retention, legal interception of communication data and on the use of DNA. UK legislation on the use of DNA shows how the proportionality principle of data protection and the necessity principle of privacy law are gradually eroding. The original intent of the legislation was to enable the collection of DNA from people arrested and charged for sexual offences or other serious crimes to the retention of DNA of people who are merely arrested (and not charged) for these crimes.

"Do not remain in the legal-technological field"

- Privacy is not only an issue of law and technology. More attention was needed on social and economical issues related to privacy. For example, the consent principle and margin of negotiation is de facto not strong: companies want to have and impose the same privacy policy on all their customers.
- Studies are needed on the economic value of privacy taking into account the loss of opacity and loss of control.
- People need to be made much more aware of and educated about privacy issues.

Don't under-estimate trust and over-estimate security

- Don't under-estimate the importance of trust! When building policies, we should assume that people trust governments and companies. The data retention laws, for example, were easily adopted in Europe (which was unexpected in view of the experiences of European history) and would seem to suggest that people are prepared to surrender their privacy without much objection.
- By the same token, we should not over-estimate security protections. Security is over-estimated, e.g., more people in Germany die in car accidents than in serious crimes.

From a legal point of view

- A comment was made that privacy and data protection are threatened by AmI, that they cannot exist at the same time. It is dangerous to change the principle of explicit consent to implicit consent, whereby we would rely more on a reasonable expectation of privacy protection.
- A multi-layer format or approach to the protection of information was needed. We need to categorise and/or distinguish the categories of information to be provided, for example, essential information and additional information for which explicit and prior consent is necessary before any data processing takes place.
- We should create "sticky policies", which means that you technically attach a privacy policy to personal data that would follow the collected data in any further time and any place. Such sticky policies should be supported by trust mechanisms.
- Trust labels should be created.
- Mark Weiser stated that the most profound technologies are those that disappear into the background. Similarly, you can make the law very strong and make it disappear into the background, but it would always be there. Further thought needs to be give to how can this be done.
- Responsibilities for data protection should be clearly indicated and should take into account the user in line with the OECD's 2002 Security Guidelines.

Martin Meints observed that privacy management (such as proposed in the PISA and PRIME projects) is not always possible. Privacy management might work where

a user can communicate with the environment through a device under his control and which has hisprivacy-settings, but not in an environment where passive authentication through biometrics takes place.

John Borking, the chair of the panel discussion, asked where our information society is going. Are we being pushed into conformity? Is our information society really one without privacy? Is it a society where the individual's identity and subjectivity are given up for the sake of the collective society, collective intelligence, AmI?

Session 2 – Security in a world of ambient intelligence

Michael Friedewald

Fraunhofer Institute Systems and Innovation Research, Breslauer Straße 48, 76139 Karlsruhe, Germany, Michael.Friedewald@isi.fraunhofer.de

The following issues, policies and safeguards were presented and discussed in the seession on security and security safeguards. Presentations were given by Mario Hoffmann, Andreas Pfitzmann, Stephan Engberg, Reinhard Schwarz, Charles Raab and Achilles Kameas.

What should be the basis of security?

- One participant suggested in his talk that (security in) modern society is based not on trust but on distrust
- In the discussion, this premise was vehemently questioned by other participants. No agreement could be reached on this topic.
- This premise has a couple of implications and consequences for a security concept of AmI:
  - It has to be made sure that unnecessary personal data cannnot be collected.
  - For this purpose, each individual should have a trusted personal device that is the only means for communication with other individuals and the environment. This device must not be identifiable by an analogue radio signal (which is the case today).
  - Since the personal device is crucial, personal data on the device should be protected with the best crytographic methods available.
  - Sensor abilities to sense human beings from a distance should be minimised.
- According to another presentation, today's security paradigm is destructive, since growing risks lead to more security needs, which leads to more identification needs and the collection of more data which creates new (more) risks.
- Since central control eventually leads to less (or even zero) security, data should be kept as local as possible, remaining in the context where it was created and under the control of the subject it describes.
- One proposed solution for RFIDs was to change their behaviour depending on the context where they are used. When products are still in the producer's or retailer's distribution chain, the tag's behaviour should have a different behaviour from that in purchasing activities where customers are involved.

There is a general need for Privacy Impact Assessments

One panelist spoke in favour of a systematic "Privacy Impact Assessment" with an emphasis on risks on the basis of the precautionary principle. Many influential scenarios either fail to identify crucial points in assessing privacy issues or only offer a "toolkit" of countermeasures.

Safeguards should be designed on the basis of a holistic approach, since in most cases a combination of safeguards is needed. In any case, roles, relationships and responsibilities in an AmI world seem more important than the gizmos of technological possibilities. The important questions for Privacy Impact Assessment are "Who should do what, when and especially why?"

Biometrics will not be the basis of more security

Several presenters and participants argued that biometrics is *not* the solution for security problems in a AmI world, since the identification and authentication of individuals by biometrics will always be approximate, is like publishing passwords, can always be spoofed and cannot be revoked after an incident.

How can security be implemented in complex and distributed systems

- One panellist addressed the question how – once security requirements have been defined – a system can be implemented that does what it is intended to do without producing new security holes.
- Though there exist many solutions to address particular security problems, no model for the security management of whole systems has emerged. This is due to many conflicting goals like invisibility vs. access control, location based services vs. location privacy, authentication vs. anonymity needs, etc., which cannot be solved with current software engineering techniques.
- One major problem is how to address dynamically changing systems, where trivial changes can radically alter system security.
- The challenge for software enngineering is to develop AmI systems where components entering the system contribute incrementally to the validity and security of the system.

"Digital Territories" – a new concept for thinking about security and privacy in an AmI world

Achilles Kameas presented the concept of "Digital Territories" (DT) as a novel way of thinking about the Ambient Intellligence world. The DT concept was developed by Beslay and Hakala [1] and explored by a study for the IPTS. It is an attempt to make the "old and well-known concept of territory a useful analogue for thinking about AmI. In general, proximity in DT is the substitute for continuity in physical space. Privacy in DT is enabled by the definitions of boundaries and/or "bubbles". Crossing the boundaries and transmitting data can be negotiated depending on the

context of the application and the owner of the DT. Though there is no empirical evidence for the practicality of the DT concept, session participants regarded it as an interesting possibility.

References

[1] Beslay, L. and Hakala, H. (Forthcoming in 2006). Digital territory: Bubbles. In Wejchert, J., editor, *The Vision Book*. Brussels.

Session 3 - The digital divide in a world of ambient intelligence

David Wright

Trilateral Research & Consulting, 12 Tybenham Road, SW 19 3LA London, United Kingdom, david.wright@trilateralresearch.com

The session on digital divide in a world of ambient intelligence was chaired by Michael Rader from the Institute for Technology Assessment and Systems Analysis, Germany. There were five presentations, with questions, answers and discussion following each. Key points from the session were as follows.

The first presenter was *Jeffrey Burke* from the University of California at Los Angeles, whose remarks were on "Discovery, expression and responsibility: Design dimensions for ambient intelligence". He referenced some of the multidisciplinary collaboration at UCLA which sought to involve artists, engineers and citizens and a broad range of AmI technologies and, in particular, networking sensors. One aim of the research in which he was engaged has been to explore the possibilities for artwork supported by technology in an urban context. He said four divides have been encountered, which prompt certain questions as follows:

Access: If the claim of ubiquity is not fulfilled, are we still speaking of ubiquitous computing?
Relevance: Whose ubiquity for which ends?
Design: Who defines the services?
Transparency: How should technology make obvious how it actually collects sensor data?

Jeff said task efficiency should not be the only design priority, especially for applications with expressive purposes. An alternative is discovery as a design priority. Without exploration of possibilities, self-reflexivity suffers. Jeff said visualisation was an important issue – i.e., it was desirable to make it apparent to "users" in an ambient intelligence environment how systems work (in a readily comprehensible way) in order improve understanding of technology and the possibilities thereof.

In the discussion following his remarks, Jeff said that SWAMI had referred to the *Embedded Everywhere* report [1] in its summary pre-conference paper, but he also encouraged SWAMI to review the *Beyond Productivity* report [2], published by the National Academies Press in 2003, which encouraged the involvement of artists with engineers in collaborative embedded research. He mentioned projects in which UCLA was involved, one of which used RFIDs in a city square. One project was

aimed at letting local people register electronically their stories or recollections of the local community. He emphasised the need to understand the technological tools for authoring and the balance between privacy and expression. In his view, the dark side of ambient intelligence was the opacity of the so-called disappearing computer phenomenon.

In response to a question, he said that the US was still at least five years away from serious commercial application of embedded systems. Such networks have application for supporting the arts and education.

Lutz Kubitschke from Empirica, Germany, gave a presentation on "Policies for an inclusive Europe". He is co-ordinator of the "e-inclusion@EU" project, the focus of which was on e-inclusion policies and initiatives. There was not a special focus on AmI, rather the focus was more broadly on information technologies and their applications, which confront citizens every day. Some people have access to these technologies and some don't. He distinguished between the first and second orders of digital divide, where the first order related to the physical unavailability of AmI networks while the second order related to factors that inhibited access to such networks once they were available. Such factors could be disabilities or inadequate income or educational level.

He said the debate on digital divide these days centred not so much on reducing the number of "outs", but increasingly on enabling users to take advantage of technology. The policy perspective was focused on countering exclusion, exploiting opportunities and promoting inclusive developments. The digital divide issue was the subject of many activities at all levels of government in numerous policy fields (It's a complex policy area). Most of today's policies are also relevant for an AmI future – but the emphasis is on the "second order divide" which could include the participatory shaping of the AmI environment.

E-inclusion policies and initiatives could be considered in the context of four principal factors, namely access (location, quality), accessibility (access tools, content), usability (access tools & content) and appropriateness (relevance, access tools). Efforts were needed to make sure that everyone is included in the knowledge-based society, which frames European policy. The diversity of stakeholders makes the policy "space" quite complex.

Lutz said he felt the SWAMI dark scenarios were very useful. When the e-inclusion project was started, AmI was not really considered, but the SWAMI scenarios have prompted consideration of the issue. As more government services go online and people are referred to websites for more information, excluded people, those without access, obviously have a more difficult time.

Dimitris Gritzalis from the Economic and Business department of Athens University gave a presentation on "Ambient Intelligence: Promise, Price, Social Disruption: A Review of Security and Privacy Strategies in Leading Economies", which essentially compared the AmI approaches (a.k.a. pervasive computing, ubiquitous networking) of the EU, the US and Japan. He said Japan was focused on developing strategic superiority, ensuring Japan's industrial lead. The US was preoccupied with security, especially since 9 September 2001, and preserving its technological competitiveness. Cyber security and co-ordinated approach to homeland security would

continue to underpin US efforts in this area. The EU was exploring new opportunities, e-government services and civil security. The EU's seventh framework programme would be oriented towards security and fundamental rights. The ITU was also looking at ubiquitous networking issues. We needed to pay attention to how China, Brazil and India dealt with AmI.

Prof Gritzalis summarised his comparisons in the following way. He remarked that the European Union

- is optimistic of AmI, but does not disregard the fact that people will participate in a multiplicity of parallel, overlapping, inter-leaved and evolving one-to-one, one-to-many and many-to-many relationships, some short-lived, and some established temporarily and instantaneously;
- is oriented towards addressing different security aspects, such as security related to the individual, to communities and social groups, to the industry or to critical infrastructures;
- builds citizens' confidence in AmI spaces, by facing privacy issues, unfair or illegal commercial practices, unsolicited communications, and harmful content distribution;
- has adopted AmI as its emerging ICT paradigm and aims to exploit its leading position in wireless and mobile technology;
- wishes to adopt a holistic view of AmI, considering "not just the technology, but the whole of the innovation supply-chain from science to end-user, and also the various features of the academic, industrial and administrative environment that facilitate or hinder realisation of the AmI vision".

The US, said Prof Gritzalis,

- considers it important to analyse not only technological issues, but also social and ethical issues;
- aims at promoting interdisciplinary approaches to research on UbiComp, which tie computer science with other sciences and disciplines;
- considers that UbiComp introduces a new security paradigm, regarding how we deal with novel and sophisticated security and privacy requirements, recognising that technical approaches will be insufficient for the protection of privacy and security in UbiComp;
- from the national security perspective, is probably the most organised nation in the world, in terms of strategies adopted and actions taken;
- aims at keeping its leadership in the ICT sector, while preserving national security, through concepts such as cyber security and critical infrastructure protection;
- undertakes initiatives often addressing issues such as patient safety and health, quality, prediction of health effects of pollutants, and participation in the digital society, but with no high priority.

Japan, finally,

- aims at "being different" with UbiNet, while it expects to "learn from the advanced and comprehensive" security-related approaches taken in the US;

- adopted UbiNet not only as its emerging ICT paradigm, but also as a main means for making the country the "leading ICT nation in the world";
- aims at being the "most safe and secure" nation in the world in the next decade or so, and to take care of the elderly, the disabled and working women;
- does not focus on pressing victims to take appropriate preventive measures but on punishing perpetrators of attacks. Thus the focus should be on the prosecution of offenders;
- follows the tradition of the "three sacred treasures" of ubiquitous home appliances, ubiquitous offices and ubiquitous cars.

In the discussion that followed his remarks, the comment was made that while there were some differences in approaches and rationales, the EU, the US and Japan had similar concerns re national security, benefits to civil society, industrial competitiveness in the context of AmI.

Michael Huch from VDI/VDE Innovation + Technik, Germany, presented remarks on "Ambient Assisted Living: Preparing a European RTD Programme". The Ambient Assisted Living project was a preparatory action for a European RTD programme. The idea is to initiate an Art 169 research programme in 2007, with a budget of EUR 700 million budget over seven years, with funding from Member States, EC and industry. Calls for proposals will be based on strong user involvement (a safeguard) in defining objectives & projects. AAL aims at prolonging time people can live in a decent way in their home environment. Michael Huch posed the question: At which level in the value chain are SWAMI issues best dealt with?

The final presenter in the digital divide session was *Rob van Kranenburg* from Resonance Design in Belgium whose remarks were on "Distributing insecurity". Rob posed a trust paradox, that is, why should I distribute myself as data if I'm told the environment is untrustworthy? Among other things, his remarks addressed sensor-based innovation. He said digital networks were turning ordinary citizens into amateur professionals. He described RFID technology's measure of success as the extent to which it disappears, perhaps the first time a measure of success is the extent to which it disappears. Unlike other networks, he said, AmI is not driven by a focus on control (a manifestation of which is proprietary technology), a notion we needed to let go of. A reflection of this letting go of control was a phenomenon he described as distributing insecurity or, to put it differently, perhaps we should make the EU a security free zone.

In the discussion that followed his presentation, there were some comments that in Europe our capitalism is based on service, to make a security-free zone, we should publish ideas and concepts on the Web, so that a company can't patent an idea, which should have wide currency. In the AmI world, a new business model may be needed where the focus is on provision of services based on competition, rather than development of proprietary technologies.

Cultural issues need to be considered in the context of AmI. There was some discussion also of who will pay for AmI infrastructure?

One participant in the session noted that, at this conference, the digital divide panel session had the smallest room and smallest number of participants, which showed that the digital divide issue needs a higher priority.

At the end of the day, an important question remains: will AmI help overcome the digital divide or will AmI deployment broaden the digital divide?

References

[1] Estrin, D., editor (2001). *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers*. National Academies Press, Washington, D.C.

[2] Mitchell, W. J., Inouye, A. S., and Blumenthal, M. S., editors (2003). *Beyond Productivity: Information Technology, Innovation, and Creativity*. National Academies Press, Washington, D.C.

Panel discussion: Policy Options

Ioannis Maghiros

European Commission, DG JRC, Institute for Prospective Technological Studies (IPTS), Edificio Expo, C/ Inca Garcilaso, s/n, 41092 Sevilla, Spain,
Ioannis.Maghiros@cec.eu.int

The last part of the SWAMI conference featured a panel which debated policy options to address the issues raised during the SWAMI conference. The panel was composed of Peter Hustinx, the European Data Protection Supervisor; Alain Esterle, Head of the Technical Department at ENISA (European Network and Information Security Agency), Jacques Bus, Head of Unit on "ICT for Trust and Security"; Andrea Servida, deputy Head of Unit on "Internet, Network and Information Security"; and Inmaculada Placencia-Porrero, deputy Head of Unit "eInclusion".

1. While the SWAMI proposed "dark scenarios" could be used to extrapolate average solutions for an average public, there are groups in society that are confronted by a harsher reality than that depicted in the SWAMI dark scenarios.
2. There are specific research requirements that need to be addressed, mostly related to known market failures (eIdentity, e-signatures etc.).
3. Network and information security policy requires that improved policy frameworks be created to deal with all sorts of problems, including spam and spyware or cyber crime in general.
4. There is a need to balance opportunities and risks in this new emerging environment. Risk anticipation is fundamental for our post-liberal values society. Pro-active advice on new legislation is required as is a process to trigger the responsibility of market players.
5. It is important to reconsider the participation of stakeholders in policy consensus debates and to come up with a more open method to identify in what way the market's playing field could be levelled.
6. The whole issue of privacy protection should go beyond data protection and empower the individual to intervene in the classical industry/government power struggle. A way forward could include imposing certified secure products.
7. Anti-discrimination objectives would have to figure higher in the AmI agenda.

Part IV

Appendix

List of Participants

Emile Aarts
Philips Research
Building WOp.104
High Tech Campus 36
5656 AE Eindhoven, The Netherlands
emile.aarts@philips.com

Petteri Alahuhta
VTT Electronics
Kaitoväylä 1
FIN 90571 Oulu, Finland
Petteri.Alahuhta@vtt.fi

Loretta Anania
European Commission
DG INFSO - F1 (BU33 3/71)
200 Rue de la Loi
B - 1049 Brussels, Belgium
Loretta.Anania@cec.eu.int

Laurent Beslay
European Data Protection Supervisor (EDPS)
Rue Wiertz, 60
B - 1047 Brussels, Belgium
lbeslay@edps.eu.int

John Borking
Borking Consultancy
Lange Kerkdam 27
2242 BN Wassenaar
The Netherlands
jborking@xs4all.nl

Michael Boronowsky
University of Bremen
Center for Computing Technologies (TZI)
P. O. Box: 33 04 40
D-28334 Bremen, Germany
mb@tzi.de

Maarten Botterman
RAND Europe
Newtonweg 1
2333 CP Leiden, The Netherlands
maarten@rand.org

Frans de Bruïne
European Commission
DG INFSO - H (BU33 7/66)
200 Rue de la Loi
1049 Brussels, Beglgium
frans.de-bruine@cec.eu.int

Jeffrey Burke
University of California at Los Angeles
Center for Research in Engineering, Media and Performance
102 East Melnitz Hall
Los Angeles, CA 90095-1622 USA
jburke@hypermedia.ucla.edu

Jacques Bus
European Commission
Information Society & Media DG; D4
jacques.bus@cec.eu.int

Johann Cas
Austrian Academy of Sciences
Institute for Technology Assessment
Strohgasse 45
A-1030 Vienna, Austria
jcas@oeaw.ac.at

Sabine Delaitre
European Commission, DG JRC
Institute for Prospective Technological Studies (IPTS)
Edificio Expo, C/ Inca Garcilaso, s/n
41092 SEVILLA, Spain
Sabine.DELAITRE@cec.eu.int

Sari Depreeuw
Vrije Universiteit Brussel
Faculty of Law, Law Science Technology & Society (LSTS)
Pleinlaan 2
1050 Brussel, Belgium
Sari.Depreeuw@vub.ac.be

Stephan Engberg
Priway
Stengaards Alle 33D
2800 Kgs. Lyngby, Denmark
Stephan.Engberg@priway.com

Alain Esterle
European Network and Information Security Agency (ENISA)
P. O. Box 1309
71001 Heraklion – Crete, Greece
Alain.Esterle@
enisa.eu.int

Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research (ISI)
Breslauer Strasse 48
76139 Karlsruhe, Germany
m.friedewald@
isi.fraunhofer.de

Catarina Frois
University of Lisbon, Institute of Social Sciences
Avenida Professor Aníbal de Bettencourt, 9
1600-189 Lisbon, Portugal
catarina.frois@ics.ul.pt

Dimitrios Gritzalis
Athens University of Economics & Business
Dept. of Informatics
76 Patission Ave.
Athens GR-10434, Greece
dgrit@aueb.gr

Serge Gutwirth
Vrije Universiteit Brussel
Faculty of Law, Law Science Technology & Society (LSTS)
Pleinlaan 2
1050 Brussel, Belgium
serge.gutwirth@vub.ac.be

Paul de Hert
Vrije Universiteit Brussel
Faculty of Law, Law Science Technology & Society (LSTS)
Pleinlaan 2
1050 Brussel, Belgium
paul.de.hert@vub.ac.be

Mario Hoffmann
Fraunhofer-Institute for Secure Information Technology (SIT)
Rheinstrasse 75
64295 Darmstadt, Germany
Mario.Hoffmann@
sit.fraunhofer.de

Wide Hogenhout
European Commission
DG INFSO - F1
B - 1049 Brussels, Belgium
Wide.hogenhout@cec.eu.int

Gus Hosein
The London School of Economics and Political Science
Department of Information Systems
Houghton Street, London WC2A 2AE, United Kingdom
i.r.hosein@lse.ac.uk

Michael Huch
VDI/VDE Innovation + Technik GmbH
Steinplatz 1
10623 Berlin, Germany
Huch@vdivde-it.de

Jan Huizenga
TNO Information and Communication Technology
P. O. Box 5050
2600 GB Delft, The Netherlands
J.Huizenga@telecom.tno.nl

Peter Hustinx
European Data Protection Supervisor (EDPS)
Rue Wiertz, 60
B - 1047 Brussels
phustinx@edps.eu.int

Achilles Kameas
Hellenic Open University
23 Sahtouri str,
26222 Patras, Greece
kameas@math.upatras.gr

Erkki Kemppainen
STAKES
Lintulahdenkuja 4
00530 Helsinki Finland
Erkki.Kemppainen@stakes.fi

Jay Kishigami
SSP SI Lab, NTT
3-9-11, Midoricho, Musashinoshi
Tokyo 180-8585, Japan
jay@ntt.net

Takashi Kobayashi
Tokai University
School of Political Science and Economics
1117 Kitakaname
Hiratsuka-shi, Kanagawa, 259-1292
Japan
tk@keyaki.cc.u-tokai.ac.jp

Rob Van Kranenburg
Resonance Design
Tentoonstellingslaan 22
9000 Gent, Belgium
kranenbu@xs4all.nl

Lutz Kubitschke
empirica GmbH
Oxfordstr. 2
D - 53111 Bonn, Germany
Lutz.Kubitschke@
empirica.com

Marc Langheinrich
Swiss Federal Institute of Technology Zurich
Inst. for Pervasive Computing
Clausiusstr. 59
8092 Zurich, Switzerland
langhein@inf.ethz.ch

Ralf Lindner
Fraunhofer Institute for Systems and Innovation Research (ISI)
Breslauer Strasse 48
76139 Karlsruhe, Germany
r.lindner@
isi.fraunhofer.de

Juliet Lodge
University of Leeds
Jean Monnet European Centre of Excellence
R4eGov programme, Institute of Communication Studies
Leeds, LS2 9JT, United Kingdom
j.e.lodge@leeds.ac.uk

Michael Lyons
BTexact Technologies
Antares 2 PP7, Adastral Park, Martlesham Heath
Ipswich, IP5 3RE, United Kingdom
michael.h.lyons@bt.com

Gary T. Marx
Massachussetts Institute of Technology
Cambridge, USA
Postal address:
6209 E. Kelton Lane
Scottsdale, AZ 85254, USA
gtmarx@garymarx.net

Ioannis Maghiros
European Commission, DG JRC
Institute for Prospective Technological Studies (IPTS)
Edificio Expo, C/ Inca Garcilaso, s/n,
41092 SEVILLA, Spain
Ioannis.Maghiros@cec.eu.int

Louis Marinos
European Network and Information Security Agency (ENISA)
P. O. Box 1309
71001 Heraklion – Crete, Greece
Louis.Marinos@enisa.eu.int

Martin Meints
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
P. O. Box 71 16
D-24171 Kiel, Germany
LD102@datenschutzzentrum.de

Anna Moscibroda
Vrije Universiteit Brussel
Faculty of Law, Law Science Technology & Society (LSTS)
Pleinlaan 2
1050 Brussel, Belgium
Anna.Moscibroda@vub.ac.be

Louis Neven
Twente University
Department of Science, Technology, Health and Policy Studies (STeHPS)
P. O. Box 217
7500 AE Enschede, The Netherlands
L.B.M.Neven@BBT.utwente.nl

Marketta Niemelä
VTT Technical Research Centre of Finland
P. O. Box 1300
33101 Tampere, Finland
marketta.niemela@vtt.fi

Andreas Pfitzmann
Dresden University of Technology
Department of Computer Science, Institute for System Architecture
01062 Dresden, Germany
pfitza@inf.tu-dresden.de

Olli Pitkänen
Helsinki Institute for Information Technology
P. O. Box 9800
02015 TKK, Finland
olli.pitkanen@hiit.fi

Inmaculada Placencia-Porrero
European Commission
DG INFSO - H3
B - 1049 Brussels, Belgium
inmaculada.placencia-porrero@cec.eu.int

Charles Raab
The University of Edinburgh
School of Social and Political Studies
Adam Ferguson Building, George Square
Edinburgh EH8 9LL, Scotland, UK
c.d.raab@ed.ac.uk

Silvia Portesi
European Network and Information Security Agency (ENISA)
P. O. Box 1309
71001 Heraklion – Crete, Greece
Silvia.Portesi@enisa.eu.int

Michael Rader
Research Centre Karlsruhe
Institute for Technology Assessment and Systems Analysis
P. O. Box 3640
76021 Karlsruhe, Germany
rader@itas.fzk.de

Bart van Rijnsoever
Philips Research
Holstlaan 4 WY 6
5656 AA Eindhoven, The Netherlands
bart.van.rijnsoever@philips.com

Martina Rohde
European Commission
DG INFSO - A3
B - 1049 Brussels, Belgium
Martina.rohde@cec.eu.int

Alexander Roßnagel
Universität Kassel, FB 7
Nora Platiel Str. 5,
34109 Kassel, Germany
a.rossnagel@uni-kassel.de

Alberto Sanna
Fondazione Centro San Raffaele del Monte Tabor
Via Olgettina 60
I-20100 Milan, Italy
Alberto.sanna@hsr.it

Wim Schreurs
Vrije Universiteit Brussel
Faculty of Law, Law Science Technology & Society (LSTS)
Pleinlaan 2
1050 Brussel, Belgium
wim.schreurs@vub.ac.be

Reinhard Schwarz
Fraunhofer Institute Experimental Software Engineering
Fraunhofer-Platz 1
67663 Kaiserslautern, Germany
reinhard.schwarz@iese.fraunhofer.de

Andrea Servida
European Commission
DG INFSO - A3
B - 1049 Brussels, Belgium
Andrea.Servida@cec.eu.int

Bibi van den Berg
Erasmus University Rotterdam, Faculty of Philosophy
P. O. Box 1738
3000 DR Rotterdam, The Netherlands
vandenberg@fwb.eur.nl

Elena Vildjiounaite
VTT Electronics
Kaitoväylä 1
FIN 90571 Oulu, Finland
Elena.Vildjiounaite@vtt.fi

David S. Wall
University of Leeds
Centre for Criminal Justice Studies
Department of Law
Leeds, UK LS2 9JT, United Kingdom
D.S.Wall@leeds.ac.uk

Gabriel Waller
Nokia
Eriksnäsvägen 324
FIN-01150 Söderkulla, Finland
gabriel.waller@kolumbus.fi

Kevin Warwick
University of Reading
Department of Cybernetics
Whiteknights
Reading, RG6 6AY, United Kingdom
kw@cyber.rdg.ac.uk

David Wright
Trilateral Research & Consulting
12 Tybenham Road
SW 19 3LA London, United Kingdom
david.wright@
trilateralresearch.com

Conference Program

Tuesday 21 March 2006 – Threats and vulnerabilities posed by AmI

SWAMI Session (Chair: Ioannis Maghiros, IPTS)		
9:00	Welcome address	Frans de Bruïne, director, DG INFSO
9:15	Safeguards in a world of ambient intelligence: Introduction to the project	Michael Friedewald, Fraunhofer ISI, Germany
9:35	Overview of SWAMI findings on threats, vulnerabilities and safeguards	David Wright, Trilateral
9:55	Questions and Answers	

Keynotes		
10:00	Wiring in Humans – advantages and problems as humans become part of the machine network via implants	Kevin Warwick, Reading University, UK

11:00 Coffee Break

Keynotes (continued)		
11:30	Mr. Rocky Bottoms Encounters 35 Techno-Fallacies: a Fictional Speech and Critical Analysis	Gary T. Marx, Massachusetts Institute of Technology, USA

12:30 Lunch Break

Parallel Sessions	
14:00	Session 1 – Privacy safeguards in a world of ambient intelligence
14:00	Session 2 – Security in a world of ambient intelligence
14:00	Session 3 – The digital divide in a world of ambient intelligence

15:00 Coffee Break

Parallel Sessions (continued)		
15:30	Panel Discussion 1 – Privacy safeguards in a world of ambient intelligence	
15:30	Panel Discussion 2 – Security in a world of ambient intelligence	
15:30	Panel Discussion 3 – The digital divide in a world of ambient intelligence	
17:30	Closing Remarks day 1	Ioannis Maghiros, IPTS

20:00 Conference Dinner

Parallel Session 1 – Privacy safeguards in a world of ambient intelligence

14:00	Presentations	Chair: John Borking, Borking Consultancy, The Netherlands
	Combating Criminality in a World of Ambient Intelligence	Gus Hosein, London School of Economics, United Kingdom
	AmI – The European Perspective on Data Protection Legislation and Privacy Policies	Martin Meints, Independent Centre for Privacy Protection, Germany
15:30	Panel Discussion	Chair: John Borking, Borking Consultancy, The Netherlands
	Privacy in pervasive computing environments – A contradiction in terms	Johann Cas, Institute for Technology Assessment, Austria
	Building privacy-aware AmI systems	Marc Langheinrich, ETH Zurich, Switzerland
	Privacy Incorporated Software Agents	Jan Huizenga, TNO, The Netherlands
	Enhancing trust by implementing Identity Assurance	Maarten Botterman, RAND Europe, The Netherlands

Parallel Session 2 – Security in a world of ambient intelligence

14:00	Presentations	Chair: David S. Wall, University of Leeds, UK
	Security concerns as viewed by the Wireless World Research Forum	Mario Hoffmann, Fraunhofer Institute for Secure Information Technologies, Germany
	Anonymity, unobservability, pseudonymity and identity management requirements for an AmI world	Andreas Pfitzmann, Technical University Dresden, Germany
15:30	Panel Discussion	Chair: David S. Wall, University of Leeds, UK
	Empowerment and Context Security as the route to Growth and Security	Stephan Engberg, Priway, Denmark
	Security requirements in the context of AmI systems	Reinhard Schwarz, Fraunhofer Institute Experimental Software Engineering, Germany
	Some privacy-related aspects of surveillance in the UK	Charles Raab, University of Edinburgh, United Kingdom
	Security concerns associated with digital territories	Achilles Kameas, Hellenic Open University, Greece

Parallel Session 3 – The digital divide in a world of ambient intelligence

14:00	Presentations	Chair: Michael Rader, Research Centre Karlsruhe, Germany
	Discovery, expression and responsibility: Design dimensions for ambient intelligence	Jeffrey Burke, University of California at Los Angeles, USA
	Policies for an inclusive Europe	Lutz Kubitschke, Empirica, Germany
15:30	Panel Discussion	Chair: Michael Rader, Research Centre Karlsruhe, Germany
	AmI: The Promise, the Price and the Social Disruption	Dimitris Gritzalis, Athens University of Economics and Business, Greece
	Ambient Assisted Living - Preparing a European RTD Programme	Michael Huch, VDI/VDE Innovation + Technik, Germany
	Distributing insecurity	Rob van Kranenburg, Resonance Design, Belgium

Wednesday 22 March 2006 – Safeguards and Policy options

SWAMI Session		
9:00	Rapports of parallel sessions	Michael Friedewald, Wim Schreurs, David Wright
9:30	SWAMI Dark scenarios	Ioannis Maghiros, IPTS, Spain
9:50	SWAMI Legal aspects	Paul De Hert, Vrije Universiteit Brussel, Belgium
10:10	Questions and Answers	

10:30 Coffee Break

Plenary Session		
11:00	Use of RFID in Ambient Intelligence: critical issues for policy makers	Jay Kishigami, NTT, Japan
11:30	Ambient Intelligence: New ways of innovation for Europe	Emile Aarts, Philips, The Netherlands
12:00	Panel discussion: Policy Options - Peter Hustinx, European Data Protection Supervisor - Andrea Servida, European Commission, DG INFSO A3 - Jacques Bus, European Commission, DG INFSO D4 - Alain Esterle, European Network and Information Security Agency - Inmaculada Placencia-Porrero, European Commission, DG INFSO H3	
13:00	Closing Remarks	Ioannis Maghiros, IPTS

Deliverable Summary Sheet

Project Number:	IST-2004-006507
Project Acronym:	SWAMI
Project title:	Safeguards in a World of Ambient Intelligence
Deliverable no.:	5
Due date:	July 2006
Delivery date:	Draft version, April 2005
Delivery status:	Public
Work package no.:	4
Leading partner:	Fraunhofer ISI (Project co-ordinator), Trilateral Research & Consulting (Work package leader)
Contributing partners:	All
Partners owing:	All
Distribution Type:	Public