Safeguards in a World of Ambient Intelligence[*]

Outline of a research agenda on the European Level

Michael Friedewald

Fraunhofer Institute Systems and Innovation Research, Breslauer Straße 48,
D-76139 Karlsruhe, Germany
m.friedewald@isi.fraunhofer.de

Abstract. Ambient Intelligence is a vision of the future information society stemming from the convergence of ubiquitous computing, ubiquitous communication and intelligent user-friendly interfaces. Beyond the possible benefits that are associated with this vision, it also requires a proper balance of a complex diversity of interests and values. The paper gives an outline of the various risks and vulnerabilities associated with Ambient Intelligence and argues why the design of safeguards and privacy enhancing mechanisms is a central task of European policy.

1 The Brave New World of Ambient Intelligence – Promises and Fears

Ambient Intelligence (AmI) has been described and characterised in a variety of ways and using a variety of terminologies. Pervasive computing, ubiquitous computing, embedded intelligence, invisible computing, seamless intelligence are just a few of the terms that have been used synonymously with Ambient Intelligence. Some have described the capabilities of AmI by the construction of scenarios and created roadmaps to indicate how we can arrive at such scenarios and the multi-faceted benefits that are expected to arise from the deployment of Ambient Intelligence [1, 2].

While the European Commission has supported and continues to support many projects that will help society reach this wondrous new world, in fact, the construction of the Ambient Intelligence environment has already begun. Sensors and actuators, key AmI technologies, have been in use for decades as a result of the exponential increase in electronic capabilities. However, the dramatic reduction in the cost of computing and communications and the rise of the Internet have facilitated the exchange of information among these early AmI devices and have contributed to laying the foundations for the scenarios envisaged for the future. Above all, the networking of the proliferating devices in recent years demonstrates that the future, despite the still remaining formidable technological challenges, is not so far off.

While the technologists have been at work concerns relating to privacy, security, identity, social inclusion and other issues are beginning to get more attention. The fears

[*] This paper outlines the objectives of the Project "Safeguards in a World of AMbient Intelligence (SWAMI), funded by the European Commission under Priority 8.1 (Policy Oriented Research) of the Sixth Framework Programme.

D. Hutter and M. Ullmann (Eds.): SPC 2005, LNCS 3450, pp. 63–69, 2005.

conjured up by the impact of an Orwellian Big Brother only complicate the apparent lack of trust, which hinders the full flowering of the Internet for e-commerce, e-government, e-health and much else. In November 2003, some 30 privacy advocacy groups joined together to produce a position paper calling for a halt to the deployment of radio frequency identification tags (RFIDs) until certain public policy issues are resolved [3]. After a fashion, their concerns reflect a few of the more numerous and even more complex issues raised by the IST Advisory Group (ISTAG) in their June 2002 paper entitled *Trust, dependability, security and privacy for IST in FP6* [4].

2 Challenges for European Policy

AmI should be seen as a set of artefacts requiring a proper balance which takes into account a complex diversity of interests and values related to access to information, protection of the individual sphere, trust, security, protection against discrimination, protection of identity, free speech, protection against intrusions and so on. Such a balance demands an approach which is not only driven by one or two actual, emotional, economic or social signals or events, but which proceeds by a rational mobilisation of the many possible relevant perceptions and definitions of the issues at stake. Such a balancing exercise raises a number of issues that need to be taken into account, e. g.,

- the increasing concern for security after 11 September 2001;
- technological innovation, its dissemination and consequences, only some of which can be foreseen (the invisibility of networked "intelligent" devices, ubiquity of computer communications, anonymity and privacy impacts, user friendliness, price, accessibility, etc.);
- a tendency toward privatisation of governance (the weakening of public power to control and steer the evolutions as a result of the increasing power of private actors both at local and global level).

Every one of us goes through life playing many different roles, which in essence could be reduced to three main ones Ð that of the private individual, the professional and the public participant.

Private individuals are mindful of their pursuits and/or responsibilities as parents or members of a family or on their own who from time to time have concerns about their health or modes of entertainment and leisure activity or shopping or whatever. Living in a world of Ambient Intelligence should reduce the time it takes to pursue these things and increase the richness of daily experience [5]. Similarly, the professionalÕs ability to communicate with his/her peers, either in the same office or on the other side of the world, to have an infinite world of information and intelligence at a fingertip to facilitate decision-making, will expand with Ambient Intelligence. In their public role, citizens will participate in social and political activities, perhaps lobbying for or supporting this or that cause. In each of these roles, the citizenÕs level of trust and confidence in supporting technology and in those with whom (s)he might be in contact will vary.

CitizensÕ demands for security, privacy, confidentiality, anonymity will also vary according to the situation, and the situations may be very fluid, changing many times in the course of a day. In some of their roles, they will place demands on others, in others, they must place demands on themselves or accept certain responsibilities. In some roles and at some times, they will provide consent to others, at other times, they will seek consent (access) and at still other times, they may be unaware of the computing, monitoring, networking going on around them. At all times, they must be alert to the possibility of social engineering and threats to their space, to their digital, if not their physical well-being. They need verifiable assurances that they can perform their roles according to the level of security, trust, confidentiality and anonymity that they dictate.

Therefore research is needed on the responsibilities and ethics related to the new technologies and on the social, economic, legal and technological aspects of AmI, in particular addressing:

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

However policy-makers are not the only constituency challenged by these issues. Many in industry are already sensitised to the emerging social and policy challenges inherent in the deployment of Ambient Intelligence technologies. ISTAG itself comprises leading manufacturers, software developers, and service providers and has produced some very good reports and recommendations. Similarly, many European enterprises participate in standards-setting bodies, which deal with privacy and security aspects. They should also profit from the early definition of possibilities to reach a certain level of security, trust and confidentiality.

3 Ambient Intelligence Issues in the EU Policy Framework

Reaching these objectives is seen as urgent for further development of Ambient Intelligence in Europe. Moreover, they are in line with those of the IST Priority and the broader Framework Programme 6 (FP6) objectives as well as related objectives stated by the Commission, the Council and others. The Framework Programme emphasises the importance of taking the human dimension into account in Ambient Intelligence. In doing so, it echoes the *e*Europe 2005 Action Plan that says Europe should have a secure information infrastructure and, to that end, it identifies FP6 priorities as including trustworthy network and information infrastructures with an emphasis on emerging technologies like Ambient Intelligence. Research activities, are expected to take into account the 'human factor' in security [6–p. 16]. The IST 2003 report puts it even more succinctly: Instead of making people adapt to technology, we have to design technologies for people [7–p. 10].

Taking the human factor into account is crucial in the construction of safeguards in a world of Ambient Intelligence. The success of AmI will depend on how secure its use can be made, how privacy and other rights of individuals can be protected and, how individuals can come to trust the intelligent world which surrounds them and through which they move. The European Commission has acknowledged and emphasised this dependency between technology and trustworthiness on numerous occasions.

The issues raised in the context of Ambient Intelligence affect all five key areas on which current IST research is focussed [7]: The first area includes research addressing solutions for trust and confidence. The second area includes basic technologies for Ambient Intelligence, namely communication and network technologies, embedded systems, and software technologies and distributed systems. Accordingly, they need to be considered in order to determine what mechanisms, what policy options are needed to ensure trust and confidence. The third IST area deals with components and microsystems and must be considered in the context of how they further the goals of Ambient Intelligence. The same applies to the fourth area – i.e., knowledge and interface technologies, especially knowledge technologies, digital content, intelligent interfaces and surfaces, and to the fifth area, IST future and emerging technologies.

Across the IST Priority, special emphasis must be placed on, inter alia, measures to strengthen international co-operation. Such co-operation has already been initiated within the context of Ambient Intelligence, notably with the United States [7–p. 117]. It is therefore necessary to formulate options for the Commission and other policy-making bodies with further regard to international co-operation. In a networked world, best symbolised by the Internet, in which communications and computing capabilities know no borders, international co-operation is a must if the privacy and rights of individuals are to be protected. Many risks and vulnerabilities to Europeans emanate beyond our borders, hence social and policy options must include a global outlook. The Cybercrime Convention is an important step in this direction since its 34 signatories include more than just the UnionÕs Member States. In addition, representatives from the Commission, Member States and industry participate in many standards-setting bodies concerned with cyber security with a global perspective. Nevertheless, more initiatives are needed in that direction [4–p. 10].

The provenance of the term Ambient Intelligence is recent, although it has its precursors in the notions of pervasive computing, ubiquitous computing, and so on. As Erkki Liikanen, former Commissioner for Information Society, stated, FP5 provided important foundations for the vision of Ambient Intelligence, upon which the work in FP6 is being built [7–p. 3.]. Therefore it is high time to investigate if the research policy of recent years has produced lacunae with regard to policy development and if the scientific and industrial community has developed a hidden research agenda with priorities that are different from those considered important by policy.

The definition of safeguards for the world of Ambient Intelligence is relevant to the European policy, but its global relevance is also obvious. For example, a roundtable of security experts in 2001 identified the top ten security priorities for the next decade, with the first priority related to the "EverNet", which was their way of labelling AmI. The experts were concerned that billions of devices that are always on and always connected increase the complexity of our systems to the point where it is not possible to comprehend all of what we are using. We need to resolve issues of identity and authority when these devices conduct activities for people without human intervention, when no one is around to notice [8]. Thus, the experts were urging fast action to resolve these issues.

4 The Need of Safeguards for a World of Ambient Intelligence

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

It is urgent to consider Ambient Intelligence technologies and developments and how the rights of individuals can best be protected and to formulate adequate social and policy options. This can contribute to the European policy development. Indirectly this can also contribute to scientific and technical development projects by highlighting the policy implications of the work. It is already obvious that realising the vision of Ambient Intelligence will require more than just technology and, as has happened throughout history, especially in the last decade or so, significant technological advances almost always raise policy issues.

The new regulatory framework aims for a more secure environment for e-commerce transactions and to ensure an adequate level of consumer protection. Here it is necessary to examine the adequacy of the new framework in the context of the emerging technologies, capabilities and properties that are embedded in Ambient Intelligence. This can contribute to the strengthening of the three pillars upon which the European Union's policy for the Information Society is based and, in particular, the second pillar which is the new regulatory framework covering all services or networks that transmit communications electronically [7–Forward by Erkki Liikanen].

While the world of Ambient Intelligence will bring many benefits, trust and security should be designed into the applications rather than inserted as an afterthought into an already constructed world of smart spaces. The success will depend on the acceptability by citizens and by taking steps to minimise their concerns with regard to how it might lead to further encroachments upon their privacy, safety and security.

So far, there are some bad omens, even though embedded technology is not new. What is new is that such devices are being networked and their numbers are set to increase by orders of magnitude. That has alarmed major privacy advocacy groups who recently made a joint statement calling for a halt in the use of RFIDs until key issues are resolved. Meanwhile, companies such as Wal-Mart in the US, the Metro Group in Germany and others are proceeding with their plans for a massive increase in the use of RFIDs, even before some standards issues have been resolved.

Similarly, location aware services have prompted concerns, even though they also offer many benefits. The increasing use of GPS in mobile phones in the United States in conjunction with services such as uLocate and Wherify Wireless enables those with mobile phones to be tracked wherever they go. While helping parents to know where their children are, the risks of unwanted and unwarranted surveillance have been highlighted by privacy advocates and others. These and similar examples highlight the need for urgent research in regard to the emerging world of Ambient Intelligence and, in particular, matters of privacy, security, trust, identity and so on.

The lack of consumer trust is often cited as the reason why e-commerce (and e-health and e-government) via the Internet is far from realising its potential. Attacks via the Internet are no longer confined to big name targets such as the military or credit card companies. Even individual users' home computers are being attacked or used as the staging platform for distributed denial of service attacks. Attacks are not only becoming more numerous, they are becoming much more sophisticated. The software security firm Symantec observed that, in July 2001, Code Red spread to 250,000 systems within six hours and the worldwide economic impact of the worm was estimated to be $2.62 billion. Code RedÕs spread was fast enough to foil immediate human intervention and the ramifications were huge. In the future, experts see the emergence of hypothesized threats that use advanced scanning techniques to infect all vulnerable servers on the Internet in a matter of minutes or even seconds [9]. Such predictions undermine trust and confidence.

Addressing security issues is crucial to stimulating demand for new electronic communications services, as the Commission said in its recent Communication "Electronic Communications: the Road to the Knowledge Economy" [10–p. 13]. This will be one of the principal tasks of the new European Network and Information Security Agency (ENISA), which is expected to become a centre of excellence for cyber security matters. ENISA's creation is a welcome development, especially to the extent that its purview includes Ambient Intelligence. In its 6 June 2001 Communication on ENISA, the Commission said one of the challenges to be faced will be to avoid unacceptable vulnerabilities and integrate security into the Ambient Intelligence architectures [11–Sect. 2.3]. The definition of safeguards for Ambient Intelligence is necessary for ENISA's activities in this area.

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

There are many good points in the aforementioned ISTAG paper on "Trust, dependability, security and privacy for IST in FP6" [4]. Of particular relevance is the ISTAG proposition that "security policies in this [AmI] environment must evolve, adapting in accordance with our experiences. Such approaches may be very different from present approaches to computational security policies, but may better embody our approaches to real-world person-to-person trust policies. This is the main new feature of the new paradigm for security in AmI Space." In the future AmI world new approaches to security, trust, privacy, etc., will be required and it is urgent that such new approaches will be considered before AmI becomes a reality, otherwise we, as a society, will be faced with a future akin to trying to squeeze toothpaste back into the tube [12]. It will be difficult to embed retroactively new security and trust paradigms in AmI when those technologies have been deployed. The early definition of safeguards can contribute to the development of such new approaches.

The definition of AmI safeguards also contributes to the four lines around which the *e*Europe 2005 Action Plan is structured [6–p. 9ff.], which are, firstly, policy measures to review and adapt legislation at national and European level; secondly, implementation of policy measures supported by the development, analysis and dissemination of good practices; thirdly, policy measures will be monitored and better focussed by benchmarking of the progress made in achieving the objectives and of the policies in support of the objectives; fourthly, an overall co-ordination of existing policies will bring out synergies between proposed actions.

References

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

[2] Friedewald, M., Da Costa, O., eds.: Science and technology roadmapping: Ambient intelligence in everyday life (AmI@Life). Working paper, Institute for Prospective Technological Studies (IPTS), Seville (2003)

[3] Consumers against Supermarket Privacy Invasion and Numbering (CASPIAN): Position Statement on the Use of RFID on Consumer Products. (2003) http://www.privacyrights.org/ar/RFIDposition.htm.

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

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

[6] European Commission: *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 (2002)

[7] European Commission: IST 2003 – The Opportunities Ahead. Office for Official Publications of the European Communities, Luxembourg (2003)

[8] Center for Education and Research in Information Assurance and Security, Purdue University West Lafayette, IN: CERIAS Security Visionary Roundtable: Call to Action. (2001)

[9] Schwarz, J.: Statement of John Schwarz, President, Symantec Corporation to the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Hearing on Worms, Viruses and Securing Our NationÕs ComputersÓ. http://reform.house.gov/UploadedFiles/Schwarz-v5.pdf (2003)

[10] European Commission: Electronic Communications: The Road to the Knowledge Economy. COM (2003) 65 final, Brussels (2003)

[11] European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298 final, Brussels (2001)

[12] Beslay, L., Hakala, H.: Digital territory: Bubbles. In Wejchert, J., ed.: The Vision Book, Brussel (2005)

Erschienen in: Hutter, Dieter und Markus Ullmann (Hrsg.): Security in Pervasive Computing.
Proceedings of the Second International Conference, Boppard, Germany, April 2005.
Heidelberg, Berlin: Springer (Lecture Notes in Computer Science, 3450), S. 63-69.

Lecture Notes in Computer Science 3450

Dieter Hutter   Markus Ullmann (Eds.)

Security in Pervasive Computing

Second International Conference, SPC 2005
Boppard, Germany, April 6-8, 2005
Proceedings

Springer

Volume Editors

Dieter Hutter
German Research Center for Artificial Intelligence (DFKI GmbH)
Stuhlsatzenhausweg 3, 66123 Saarbrücken, Germany
E-mail: hutter@dfki.de

Markus Ullmann
Federal Office for Information Security (BSI)
Godesberger Allee 185-189, 53175 Bonn, Germany
E-mail: markus.ullmann@bsi.bund.de

Library of Congress Control Number: 2005922931

CR Subject Classification (1998): C.2, D.2, D.4.6, H.5, K.4.1, K.4.4, K.6.5, H.4

ISSN 0302-9743
ISBN-10 3-540-25521-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-25521-5 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11414360 06/3142 5 4 3 2 1 0