SAFEGUARDS IN A WORLD OF AMBIENT INTELLIGENCE

Ioannis Maghiros[1], Yves Punie[1], Sabine Delaitre[1], Paul de Hert[2,*], Serge Gutwirth[2], Wim Schreurs[2], Anna Moscibroda[2], Michael Friedewald[3], Ralf Lindner[3], David Wright[4], Elena Vildjiounaite[5], Petteri Alahuhta[5]

[1] Institute for Prospective Technological Studies, Spain [2] Vrije Universiteit Brussel, Belgium
[3] Fraunhofer Institute Systems and Innovation Research, Germany [4] Trilateral Research & Consulting, UK
[5] VTT Electronics, Finland

ABSTRACT

Intelligent devices embedded everywhere and inter-connected with always-on capability will enable new services and applications to emerge but also greatly magnify the risk of abuse of the exchanged data. This article will present the need to develop safeguards in order to protect valuable assets if society at large is to benefit from AmI. Since the challenge lies in identifying safeguards for threats and vulnerabilities that are yet to be defined, the dark scenarios developed by the SWAMI project (Safeguards in a World of Ambient Intelligence)[1], will be presented as a tool to help illustrate risks that need to be mediated if AmI is to be a future success story and against which safeguards will need to be drawn.

1 INTRODUCTION

Weiser[2] used the term "*ubiquitous computing*" to describe the transition beyond mainframes and desktop PCs as the third wave of computing systems in 1991. It consisted of an integrated system of advanced computing devices, intelligent interface design, and anytime, anywhere data communications. The term adopted in Europe to describe this vision is "*ambient intelligence*" a concept which places more emphasis to "human-centred computing" and to the convergence of innovations in three key technologies: ubiquitous computing and ubiquitous communication, and user interface design. In May 2000, the Information Society Technologies Advisory Group, ISTAG (1) commissioned the creation of scenarios to help explore social and technical implications of ambient intelligence.

Ambient Intelligence (AmI) therefore describes a vision of the future Information Society where 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. The expected result of AmI is ultimately a more empowered user in terms of added convenience, safety, security as well as time and cost savings. AmI technology has the potential to positively impact the way we work, move, enjoy and live.

Key AmI technologies, such as sensors and actuators, have been in use already for decades. However, many more activities in daily life, at work and in other environments, will depend on the availability of AmI devices and services. Moreover, dramatic cost reductions in computing and communications facilitate an exchange of information at a vast scale. The scale, complexity, at times incompatible nature 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. In addition, the growing autonomy and intelligence of devices and applications will have implications for product liability, security and service definition.

In short, while most stakeholders paint the promise of AmI in sunny colours, there is a dark side to AmI as well. Existing public concerns about potential abuses on trust and privacy rights can only get worst since technology is progressing faster than the policy-building process that might otherwise assuage these concerns. Identifying ways to overcome the problematic implications of the dark side of AmI is required. Research in defining and deploying various safeguards and privacy-enhancing mechanisms can be seen as critical for the adoption of AmI in Europe. These and other issues have been studied at length by the SWAMI project which has as its main objective to identify the social, legal, organisational and ethical implications related to issues such as privacy, anonymity, security and identity in the context of AmI. This has been achieved through the elaboration of 'dark scenarios' which analyse vulnerabilities and risks so as to extract useful options aimed at overcoming the identified risks. This article will

* Corresponding author: Prof. Paul De Hert, Center for Law, Science, Technology and Society Studies, Vrije Universiteit Brussel, Pleinlaan 2 Building B, B-1050 Brussels, Belgium. Paul.De.Hert@vub.ac.be Tel.: +32-2-6291398, Fax +32-2-6292662

[1] SWAMI stands for Safeguards in a World of Ambient Intelligence; the European Commission FP6 funded project has five partners (Fraunhofer ISI; IPTS–JRC; Vrije Universiteit Brussel; Trilateral Research & Consulting). The 18-month project aims at identifying a range of safeguards to the threats and vulnerabilities facing privacy, identity, security, trust and digital divide from ambient intelligence. http://swami.jrc.es.

[2] In 1991, Mark Weiser, chief scientist at the Xerox Palo Alto Research Center (PARC) in California, published a paper in *Scientific American* titled "The computer for the 21st Century" (5) introducing his vision of a third generation of computing systems to a mass readership.

briefly present the SWAMI 'dark scenarios', the identified threats, vulnerabilities and corresponding safeguards and propose options for policy making.

2 SWAMI 'DARK SCENARIOS'

Scenarios are not traditional extrapolations from the present, but offer provocative glimpses of futures that can (but need not) be realised. Scenario planning provides a structured way to get an impression of the future and to uncover the specific steps and challenges in technology that have to be taken into account when anticipating the future. The use of scenarios 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. Dark scenarios are realistic although fictional extrapolations of the future highlighting potential vulnerabilities and associated threats.

The SWAMI developed 'dark' scenarios described in Punie et al (2) are the centre piece of the SWAMI project methodology and are considered as a constructive undertaking towards realising a safe and secure AmI. 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. SWAMI scenarios are 'dark' since they include applications that go wrong or do not work as expected in the aim to highlight vulnerabilities and weaknesses and likely adverse impacts.

Such 'dark' scenarios were developed in the framework of SWAMI and required both 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. While there were a lot of novelties introduced by the intentionally created scenario scripts, 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 future challenges.

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. In other words it is the type of exercise that is likely not to occur as the assets it tries to preserve are of value mainly to the individual and therefore as a collective to society in general. Moreover, a methodological outcome of the SWAMI dark scenarios is 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.

Four dark scenarios have been elaborated that encompass individual-societal and private-public concerns. These two scenario axes have helped to reduce the virtually infinite number of possible futures that could be developed to the following four:

Dark scenario 1: A typical family in different environments – presents AmI vulnerabilities in the life of a typical family moving through different environments. It introduces dark situations in the smart home, at work and while walking during the lunch break in a park.
Dark scenario 2: Seniors on a journey – also presents a family but focuses in particular on senior citizens on a bus tour. An exploited vulnerability in the traffic system causes an accident, raising many different problems related to both travel and health AmI systems.
Dark scenario 3: **Corporate boardroom & court case** – takes a different stance, involving a data-aggregating company that becomes victim of theft of the personal data which it has compiled from AmI networks and which fuel its core business. Given its dominant position in the market, the company wants to cover this up but will face the courtroom later on. The scenario also draws attention to the digital divide between developed countries that have AmI networks and developing countries that don't.
Dark scenario 4: Risk society – portrays an AmI risk society from the studios of a morning news programme. It presents an action group against personalised profiling, the digital divide at a global scale and related to environmental concerns, the possible vulnerabilities of AmI-based traffic management systems and crowd control in an AmI environment.

3 IDENTIFIED KEY ISSUES AND THREATS

Many messages have been established from the socio-economic analysis of the different situations described in the dark scenarios. The messages are organised around key SWAMI issues and threats[3] identified in a consensual way among SWAMI partners and external experts and illustrated by the scenarios in varied situations. These are briefly mentioned below:

Dark scenarios and key issues

- **Privacy**: the scenarios show different facets of privacy invasion, such as identity theft, the little brother phenomenon, data laundering, disclosure of personal data, surveillance and risks from personalised profiling.

[3] For more details, see Friedewald et al (3).

- **Security**: the scenarios depict security issues in different contexts: security imposed for tele-work, biometrics used for authentication or identification, human factors and security, malicious attacks, security audits, back-up security measures, security risks, access control, the illusion of security and viruses.
- **Identity**: the scenarios detail different components of identity (i.e., information related to legal identity, identification, authentication and preferences) and expose consequences when identity-based data are misused, erroneously used or incompletely processed.
- **Trust**: in the scenarios, trust is raised in different connections: trust and confidence, lack of trust (loss of control, unwillingness to provide data, contextual misunderstandings) and honesty.
- **Loss of control**: in the scenarios loss of control stems from different factors, for instance, when there is a lack of trust on the part of the citizen/consumer in the AmI infrastructure and its components and also when the complexity level of AmI devices or services is too high and consequently does not enable users to get what they want.
- **Dependency**: the scenarios mainly highlight its social impacts such as: dependence on personalised filtering, on seamless and ubiquitous communications, on AmI systems (e.g., health monitoring and traffic management systems) and users' feeling of dependence and frustration when the technology does not work as expected.
- **Exclusion** (vs. inclusion): the scenarios acknowledge that equal rights and opportunities for all need to be built into the design of new technologies since they are not achieved automatically.
- **Victimisation**: the scenarios illustrate victimisation as an AmI impact by describing a disproportionate reaction based on unfounded suspicions and emphasise the difficulty in being able to act anonymously (anonymity is regarded as suspicious behaviour).

Dark scenarios and threats

- **Surveillance**: every citizen/consumer leaves electronic traces as the price of participation in the ambient intelligence society. These traces will make it possible to construct very sophisticated personal profiles and activity patterns. Although the justification for installing surveillance systems has a strong public interest dimension, i.e., for the safety and security of society, surveillance raises ethical, privacy and data protection issues. One can rightly assume that there is a clear need to delineate and define the boundaries between the private and public spheres.
- **Identity theft**: without suitable security, the AmI environment may provide malicious persons opportunities to steal identity information and to use it for criminal purposes. A new kind of crime, defined as data laundering, related to identity theft is described.
- **Malicious attacks**: every new technology is plagued by weaknesses (known and/or unknown), which threaten to serve as the backdoor for malicious attackers. Some possible consequences and impacts are considered in various scenarios.
- **Digital divide**: AmI technology has the potential (because of its foreseen user friendliness and intuitive aspects) to bridge some aspects of the current digital divide but this same technology could also widen other aspects with regard to unequal access and use.
- **Spamming**: spamming encompasses several issues such as profiling, disclosure of personal data and malicious attacks. Different facets of spamming, such as false alarms and blackmail are described in several scenarios.

4 LEGAL ANALYSIS

Applying the existing relevant European legal framework to the SWAMI 'dark' scenarios resulted in the identification of lacunae and problems in the existing European Information Society laws, which drove the development of legal safeguards addressing key pre-identified threats and vulnerabilities in Gutwirth et al (4). Among these the following peculiarities of the legal regulation of AmI should be highlighted:

1. Law is only one of the available sets of tools for regulating behaviour; others include social norms, market rules as well as the architecture of the technology (e.g., cyberspace, ambient intelligence, mobile telephony, etc.).
1. AmI technological architecture might well make certain legal rules difficult to enforce (i.e. copyrights, data protection obligations) and it might cause new problems, particularly for the new environment (spam, data-veillance) but it also has the potential to regulate by enabling or disabling certain behaviour, while law regulates via the threat of sanction.
1. Law can also regulate by influencing the development of the architecture; it is expected that in order to tackle the identified problems effectively, it is necessary to consider both law and technology simultaneously. In this case questions as to how to best achieve this need be further studied – also considering the evolving socio-economic environment.
1. As the impact and effects of the large-scale introduction of AmI in society certainly spawns a lot of uncertainties, it could also be justified to consider the application of the precautionary principle (originally established as a legal principle for environmental and health problems) to widespread AmI in society problems.
1. Europe, like in other constitutional systems, uses both opacity (i.e. the right to privacy) and transparency tools (i.e. data protection law) at the

same time. Opacity tools are available to *prohibit* certain kinds of conduct of states with respect to their citizens. They define spheres of independence where the state or private actors cannot interfere. Transparency tools on the other hand are available to *regulate* the activity of states or private powers with respect to citizens. They define the principles by which the state or (powerful) private persons using technology must regulate their conduct. Most of the challenges arising in the new AmI environment should be addressed by transparency tools (such as data protection and security measures); however some prohibitions referring to political balances, ethical reasons or core legal concepts should be considered too.

1. There is strictly speaking no central legislator in Europe competent for regulating all aspects of AmI technology. This fact or legal pluralism is no better illustrated than with the example of passports (EU is competent) and identity cards (Member States are competent). The fact of legal pluralism is not restraint to the European level, but also exists within the Member States. Legal power is shared by many institutions, i.e. the legislator, the executive, data protection authorities, boards and advisory panels, etc. The absence of a central legislator at a European and State level for regulating AmI technology can raise problems, but could also be judged as advantageous. Decision making competences delegated to independent advisory bodies such as children's rights commissioners or data protection authorities could influence developments once these bodies are invited to the policy debate and are allowed to perform their roles together with Member State or European Union legislative institutions.

In general developments of jurisprudence in this area should be closely monitored as it is by focusing on the concrete technologies and their implications and by applying opacity and transparency approaches accordingly that appropriate policy options may be developed.

5 CONCLUSIONS

As a result of the analysis of the SWAMI 'dark' scenarios, a multiplicity of threats and vulnerabilities were identified leading to numerous risks. The safeguards needed to protect us against these risks are also many and diverse. However, 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 but also consider stakeholder strategy and market rules. Consequently, it is not difficult to come up with specific safeguards but it is very difficult to identify those safeguards that are likely to have the maximum impact. Also, it is clear that safeguards thus produced will have to be often revised as risks and vulnerabilities change as society adapts and technology evolves. Safeguards identified by SWAMI are presented below classified in three categories: technical, socio-economic and legal or regulatory.

Technological safeguards related to privacy protection in the context of AmI technologies relate to anonymity, pseudonymity, unlinkability and unobservability which is a difficult task as the data owner (who control data collection) and the data originator (who would like to be in control) have conflicting requirements. An important safeguard will be related to access control processes that are unobtrusive, continuous, context-dependent and which provide multimodal authentication. Secure authentication based on zero-knowledge techniques and on minimal data storage requirements would facilitate safeguards to prevent accidental logging of sensitive data. In addition, advanced Artificial Intelligence techniques may serve as access-control safeguards by alerting over unusual patterns. There is a clear field for further research as a consequence of the above findings.

Socio-economic safeguards could include such features as: supporting and adopting open standards which could potentially address the foreseen interoperability problems in AmI space. Codes of practice for protecting privacy and ISO standards relevant to privacy and identity are also among well known safeguards. Not as well known are trust marks and trust seals which are ways of enhancing public trust as they require independent guarantors and service contracts which are less visible but legally binding. Building in features to allow privacy audits and independent institutions to supply audit certificates are also good measures. Media attention, public awareness and education are among the best safeguards against intrusions to privacy or security breaches as they tend to steer developments towards consensual solutions.

Legal/regulatory safeguards already exist but as was presented through the legal analysis AmI space raises new problems. Apart from the obvious problem of defining ways to enforce existing legislation, the regulatory framework will have to be monitored and developed. It should consider among others the following concepts: accessibility and inclusion issues, accountability, liability and audit processes. Moreover, guidelines for relevant research on the basis of SWAMI findings or other sources of risks influencing user adoption are also needed. In addition, it should be noted that public procurement is a critical tool in addressing safeguards for emerging technologies.

Overall, it should be noted that SWAMI findings should be considered as the beginning of a process through which the foreseen challenges of AmI technologies may be harnessed so that the foreseen benefits of AmI services and applications could be harvested by society.

REFERENCES

1. ISTAG scenarios, 2001, "Scenarios for Ambient Intelligence in 2010", Edited by IPTS-ISTAG, EUR 19763 EN
2. 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 – Highlighting risks and vulnerabilities". SWAMI Deliverable 2. http://swami.jrc.es/pages/documents/ SWAMI_D2_scenarios_Final_ESvf_003.pdf
3. Friedewald, M., Wright, D., editors, 2006, SWAMI deliverable D5: "Report on the Final Conference", Brussels 21-22 March 2006, http://swami.jrc.es/pages/documents/ Deliverable5-ReportonConference.pdf
4. Gutwirth, S., De Hert, P., Moscibroda, A., Schreurs W., 2006, "The legal aspects of the SWAMI project" In: Friedewald, M.; Wright, D. (Hrsg.): Safeguards in a World of Ambient Intelligence (SWAMI): Report on the Final Conference, Brussels, 21-22 March 2006, S. 17-18. http://swami.jrc.es/pages/documents/ Deliverable5-ReportonConference.pdf
5. Weiser, M. 1991. Scientific American 265,3, 94-104.

Published in:
Kameas, A. D.; Papalexopoulos, D. (Eds.): Proceedings of the 2nd International Conference on Intelligent Environments (IE '06), 5-6 July 2006, Athens. Stevenage: IET Press. ISBN 0-86341-663-2