WWW.EFMN.EU The European Foresight Monitoring Network

Constructing Dark Scenarios for Privacy Policy Formulation

Foresight Brief No. 145

Authors: David Wright david.wright@trilateralresearch.com

Sponsors: European Commission / DG Information Society and Media
Type: Field/sector specific
Organizer: B-1049 Brussels, Belgium
Duration: 2005 – 2006 **Budget:** € 399,797 **Time Horizon:** 2017 **Date of Brief:** July 2008

Purpose

In the last few decades, scenarios have provided a way of analysing the implications of alternative futures, especially as they might be impacted by new technologies. This has been no less true of ambient intelligence (AmI), which may be embedded everywhere in the not so distant future. Most of the scenarios developed by AmI enthusiasts have been rather "sunny", showing how new technologies promise to make our lives more productive and enriching. A European project called SWAMI (Safeguards in a World of Ambient Intelligence) deliberately developed "dark scenarios" to highlight the threats to privacy, identity, trust and security and inclusiveness posed by new technologies. This brief describes the SWAMI scenarios and the methodology used to construct and analyse them.

SWAMI Dark Scenarios

While most AmI scenarios paint the promise of the new technologies in sunny colours, there is a dark side to AmI as well. In a way, this dark side is inherent in the very nature of AmI, for instance, the fact that AmI technologies will deliver personalised services to users means that somewhere a lot of personal information needs to be stored about the user. That being the case, there are risks that the user's personal information can be abused, either accidentally or intentionally. These risks have been recognised by policy-makers and researchers, and were at the heart of the SWAMI project, funded by the European Commission under its Sixth Framework Programme.

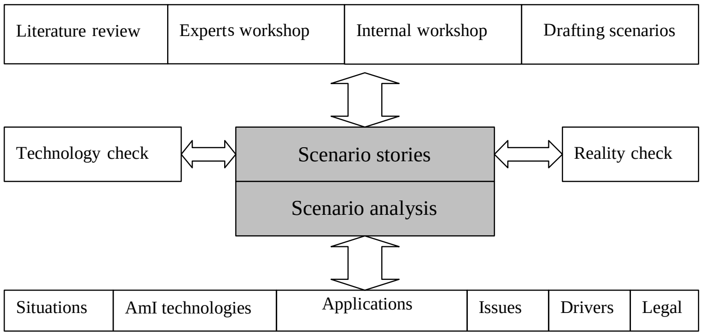
The project began in February 2005 and finished 18 months later. The SWAMI consortium had five partners: the Fraunhofer Institute for Systems and Innovation Research (Germany), the Technical Research Center of Finland (VTT Electronics), Vrije Universiteit Brussel (Belgium), the Institute for Prospective Technological Studies (IPTS, Spain) of the EC's Joint Research Centre, and Trilateral Research & Consulting (UK).

One of the tasks of the project was to create and analyse four dark scenarios that highlight the key socio-economic, legal, technological and ethical risks to privacy, identity, trust and security posed by new AmI technologies. They were called "dark scenarios", a term coined to signify things that could go wrong in an AmI world, because they present visions of the future that we do *not* want to become reality. The objective of the scenarios was to expose threats and vulnerabilities as a way to inform policy-makers and planners.

The process in constructing the scenarios began with an extensive review of existing AmI-related projects and studies. Following a workshop with other AmI experts to discuss the most important threats and vulnerabilities posed by AmI, the SWAMI partners had a brainstorming session until we agreed on the rough outlines of four contrasting scenarios. We then developed these outlines into scenario stories or scripts. To ground the scenarios in reality – to ensure that they were not too far-fetched – we did a "technology check" (are the technologies referenced in the scenarios probable?) and a "reality check" (are there press reports of events similar to those mentioned in the scenarios?). Then each partner reviewed all of the scenarios in order to eliminate doubtful points, unnecessary wordage,

The EFMN is financed by the European Commission DG Research. It is part of a series of initiatives intended to provide a 'Knowledge Sharing Platform' for policy makers in the European Union. More information on the EFMN and on the Knowledge Sharing Platform is provided at WWW.EFMN.EU

irrelevancies, etc., and to sharpen them to illustrate the points to be emphasised. Once the scenarios were "stable", we performed an analysis of them, including a legal analysis. The scenarios and associated analyses were presented at a second SWAMI workshop in order to benefit from the comments of other experts. This scenario-construction process can be depicted as follows:



The resulting four scenarios, elaborated in our book, *Safeguards in a World of Ambient Intelligence* (see the references below), are the following:

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 taking a lunch break in a park.

Dark scenario 2: Seniors on a journey – also references a family but focuses more specifically 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 – involves a data-aggregating company that becomes the victim of a theft of personal AmI-generated data that fuel its core business. Given its dominant position in the market, the company wants to cover this up but ends up in court two years later. The scenario also highlights the disparities between countries with AmI networks and those without.

Dark scenario 4: Risk society – from the studios of a morning news programme, this scenario portrays the AmI world as a risk society. 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 traffic systems and crowd management.

Elements in the SWAMI Scenario Methodology

The SWAMI consortium devised a methodology, an analytical structure for both constructing and deconstructing scenarios, not only the SWAMI scenarios, but many other technology-oriented scenarios. The analytical structure comprises the following elements or activities:

Framing the scenario

This first step summarises the scenario in question and explains its context – who are the main actors in the scenario, what happens to them, what they do, how far into the future is the scenario, where does it take place and in what domain (home, office, on the move, shopping, etc). It identifies the type of scenario (trend, normative, explorative) and key assumptions (e.g., intelligent technologies will be embedded everywhere in rich countries, but not in poor countries).

Identifying the technologies and/or devices

Next, the most important AmI technologies and/or devices used and/or implied in the scenarios are identified.

Identifying the applications

The analysis then considers the applications that emerge in each scenario and that are supported by the technologies mentioned in the previous step.

The drivers

The analysis identifies the key drivers that impel the scenario or, more particularly, the development and use of the applications. Drivers are typically socio-economic, political or environmental forces, corporate ambitions or personal motivations (e.g., greed).

Issues

Next, the major issues raised by the scenarios are identified and explicated. A discussion of the issues considered the threats and vulnerabilities exposed by the scenario, their impacts and legal implications.

Conclusions

The final step is a reality check of the scenario itself (how likely is it?) and a consideration of what should be done to address the issues it raises.

Large-scale Data Availability Multiplies Threats and Vulnerabilities

The SWAMI scenarios highlighted many of the threats and vulnerabilities that we foresee afflicting the AmI world. The principal difference (in our view) between an AmI world and that which we know today is the scale of the data available. When everything is embedded with intelligence, when AmI is pervasive and invisible, when everything is connected and linked, the threats and vulnerabilities that we know today will multiply. In an AmI world, we can expect to be under surveillance ("transparent") wherever we go because the permanent and real-time registration and processing of our presence and behaviour is the precondition – the "code" – of ambient intelligence.

The threats to our privacy, however we define it, can come from many different sources. Here are some of the principal ones that affect us today and we can assume will still be threats in an AmI world:

- hackers and attackers,
- function creep,

- surveillance,
- profiling,
- lack of public awareness or concern about privacy rights,
- lack of enforcement and oversight of privacy rights,
- erosion of rights and values,
- uncertainties about what to protect and about the costs of protection and privacy erosion,
- government and industry are less than forthright about the personal data they collect and/or how they use that data.

Is Protection Feasible? – Safeguards

The multiplicity of threats and vulnerabilities associated with AmI will require a multiplicity of safeguards. We grouped safeguards into three main approaches:

- technological,
- socio-economic,
- legal and regulatory.

Technological Safeguards – Need for Sophisticated Methods for Controlling Data Collection and Use

The main privacy-protecting principles in network applications are anonymity, pseudonymity, unlinkability and unobservability. The main difference between existing network applications and emerging AmI applications is two-fold: first, in the former case, the user has some understanding of which data about him or her are collected, and has some means to restrict data collection: e.g., to use a public computer anonymously to access certain web pages; to switch off his or her mobile phone, to pay cash instead of using a web service, etc. In the latter case, with the environment full of numerous invisible sensors (and video cameras), it is difficult, if not impossible, for users to understand and to control data collection and to achieve unobservability, anonymity and pseudonymity. Intelligent data processing, limiting linkability and implementing strong access control to collected data seem to be the main ways of protecting privacy in such applications. However, such applications present potential privacy threats anyway if the police, intelligence agencies, family members or criminals can search through devices that store personal data.

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, but physiological, video and audio sensors, proposed for AmI applications, will have much stronger capabilities to identify a person and to reveal personal activities and feelings.

Consequently, future AmI applications will require stronger safeguards, many of which are not yet fully developed. Hence, we proposed research on developing privacy-protecting safeguards such as:

- communication protocols which either do not require a unique device identifier at all or which require authorisation for accessing the device identifier;
- network configurations that can hide the links between senders and receivers of data;
- improving access control methods by multimodal fusion, context-aware authentication and unobtrusive biometric modalities (especially behavioural biometrics, because they pose a smaller risk of identity theft) and by liveness detection in biometric sensors;
- enforcing legal requirements and personal privacy policies by representing them in machine-readable form and attaching these special expressions to personal data, so that they specify how data processing should be performed, allow a privacy audit and prevent any other way of processing;
- developing fast and intuitive means of detecting privacy threats, informing the user and configuring privacy policies;
- increasing hardware and software capabilities for real-time data processing in order to minimise the lifetime and amount of raw data in a system;
- increasing software intelligence by developing methods to detect and to hide sensitive data;
- developing user-friendly means for recovery when security or privacy has been compromised.

Socio-economic Safeguards Require Cooperation

Co-operation between producers and users of AmI technology in all phases from R&D to deployment is essential to address some of the threats and vulnerabilities posed by AmI. Among the socio-economic safeguards we proposed were these:

- standards,
- privacy audits,
- codes of practice,
- trust marks and trust seals,
- reputation systems and trust-enhancing mechanisms,
- service contracts with strong privacy protections,
- guidelines for ICT research,
- raising public awareness,
- including privacy, identity and security issues in the professional education curricula of computer scientists,
- media attention, bad publicity and public opinion.

Legal and Regulatory Safeguards – Transparency Is Key

SWAMI identified some serious legal problems when applying the existing legal framework to address the intricacies of an AmI environment. We found that 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, although some prohibitions referring to political balances, ethics and core legal concepts should be considered too.

A set of rules needs to be envisaged to guarantee procedural safeguards similar to those currently applicable to the protection of our homes against state intervention (e.g., requiring a search warrant). Technical solutions aimed at defending private digital territories (the private sphere of the individual no matter where he is) against intrusion should be encouraged and, if possible, legally enforced. The individual should be empowered with the means to freely decide what kind of information he or she is willing to disclose. Such protection could be extended to the digital movement of the person, that is, just as the privacy protection afforded the home has been or can be extended to the individual's car, so the protection could be extended to home networks, which might contact external networks.

All employees should always be clearly and a priori informed about the employee surveillance policy of the employer (when and where surveillance is taking place, what is the finality, what information is collected, how long it will be stored, what are the (procedural) rights of the employees when personal data are to be used as evidence, etc.).

The status of pseudonymity under the law needs further clarification, whether pseudonyms should be regarded as anonymous data or as personal data falling under the data protection regime.

The obligation of data protection law to inform the data subject about when and which data are collected, by whom and for what purpose gives the data subject the possibility to react to mistakes or abuses, and enables him to enforce his right in case of damage. It would be desirable to provide the individual not only with information about what data are processed, but also what knowledge has been derived from the data. This might imply a rethinking of data protection law.

A means to prevent data laundering could be envisaged which would create an obligation for those who buy or otherwise acquire databases, profiles and vast amounts of personal data, to check diligently the legal origin of the data. An obligation could be created to notify the national data protection authorities when personal data(bases) are acquired. Those involved or assisting in data laundering could be subject to criminal sanctions.

Profiling practices and the consequent personalisation of the ambient intelligence environment lead to an accumulation of power in the hands of those who control the profiles and should therefore be made transparent.

Simply identifying safeguards is not sufficient, of course, so the SWAMI consortium went further and specifically addressed recommendations to the European Commission, member states, industry, academia, civil society organisations and individuals. The reader interested in more details should consult the references below.

References

Wright, David, Serge Gutwirth, Michael Friedewald et al., "Privacy, trust and policy-making: challenges and responses", *Computer Law and Security Review*, Vol. 25, No. 1, 2009 [forthcoming].

Wright, David, Serge Gutwirth, Michael Friedewald et al., *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008.

Wright, David, "Alternative futures: AmI scenarios and Minority Report", *Futures*, Vol. 40, No. 1, June 2008, pp. 473-488.

Wright, David, Michael Friedewald et al., "The illusion of security", *Communications of the ACM*, Vol. 51, Issue 3, March 2008, pp. 56-63.

Wright, David, Serge Gutwirth and Michael Friedewald, "Shining light on the dark side of ambient intelligence", *Foresight*, April 2007, pp. 46-59.