DARK SCENARIOS AS A CONSTRUCTIVE TOOL FOR FUTURE-ORIENTED TECHNOLOGY ANALYSIS: SAFEGUARDS IN A WORLD OF AMBIENT INTELLIGENCE (SWAMI)

Yves Punie, Ioannis Maghiros, Sabine Delaitre
Institute for Prospective Technological Studies, EC DG JRC, Seville, Spain

Abstract
SWAMI stands for Safeguards in a World of Ambient Intelligence. It is an FP6 funded IST 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’ as a centre piece of the SWAMI project methodology. These are realistic future scenarios which highlight threats and vulnerabilities which are subsequently analysed so as to extract useful options aimed at overcoming the identified possible risks.

The need for such scenarios stems from the fact that while most foresight scenarios have an inherent bias towards presenting mostly optimistic visions of the future, reality is never so rosy and bright. Therefore, SWAMI dark scenarios envisaged to identify and highlight possible vulnerabilities and weaknesses in order to prevent them from happening. The development of safeguards that follows from the dark scenarios is thus crucial for maintaining a constructive and realistic approach towards realising AmI in ways that are beneficial. It is also essential for achieving outcomes of the dark scenario exercise.

The aim of this paper is to discuss the SWAMI dark scenario approach as a tool for FTA. The paper will discuss the conceptual and methodological design of the dark scenarios; will provide some examples from the scenario stories and give some major outcomes in terms of highlighting threats and vulnerabilities.

Keywords: scenarios, ambient intelligence, mitigating risks, threats and vulnerabilities identification, safeguards.

THEME: FTA ASSUMPTIONS, METHODS AND APPROACHES IN THE CONTEXT OF ACHIEVING OUTCOMES

1 The views expressed in this paper are the author’s and do not necessarily reflect those of the European Commission.
1 Introduction

Ambient Intelligence (AmI) refers to a vision of the future Information Society in Europe 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. It is a vision that has been developed in Europe during the last decade, based on the idea of "ubiquitous computing" that was coined by Weiser in 1991 to describe the transition beyond mainframes and desktop PCs as the third wave of computing systems in 1991. It consists of an integrated system of advanced computing devices that become invisible but available anytime and anywhere. The idea of invisible computing has been taken-up and developed further since then in many different parts of the world according to a variety of terms: ubiquitous computing, pervasive computing, disappearing computing, pro-active computing, sentient computing, affective computing, wearable computing and ambient intelligence. The different terms may imply a different focus and also a geographical preference, hence the term AmI which is prevalent in Europe, while ubiquitous computing is more common in the USA and Japan.

Ambient Intelligence is a future vision; an emerging property that is not yet realised but based on the integrated development of current and next-generation Information Society Technologies (IST) and services: the convergence and seamless inter-operability between three key technologies: Ubiquitous Computing, Ubiquitous Communication, and Intelligent User Friendly Interfaces. (ISTAG 2001, Aarts et. al 2002; Aarts & Encarnaçoã 2006)

Ambient intelligence is seen as a key to the future information society in Europe and is promoted, amongst others, by RTD policymakers. It is a priority within the European Commission FP6 IST programme for the period 2002-2006 as well as within other pan-European and national ICT research programmes in Europe. Major steps in developing the vision of Ambient Intelligence in Europe has come from the IST Advisory Group (ISTAG), a European group of experts from industry and academia advising the IST programme. The overall vision is that the IST thematic priority contributes directly to realising European policies for the knowledge society as agreed at the Lisbon Council of 2000 and as reflected in the e-Europe Action Plan. The strategic goal for Europe in the next decade is ‘to become the most competitive and dynamic knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion’. This requires wider adoption, broader availability and an extension of IST applications and services to all economic and public sectors and society as a whole (European Commission 2002, pp.4-6).

In May 2000, ISTAG commissioned the creation of scenarios to help explore social and technical implications of ambient intelligence. This scenario exercise was launched with over 35 experts to develop a better understanding of the implications of an AmI landscape. The scenario report (ISTAG 2001) – a key reference in the field – also identified major key technologies, sociopolitical issues and a research agenda for AmI. It emphasised right from the start, the humanistic and service nature of AmI, and thus its focus on serving people, not technologies. These explicit

---

2 This paper is based on SWAMI Deliverables D2 (Punie et al. 2005) and SWAMI D3 (Friedewald, Lindner & Wright 2006).

3 In 1991, Mark Weiser, chief scientist at the Xerox Palo Alto Research Center (PARC) in California, published a paper in Scientific American entitled “The computer for the 21st Century” introducing his vision of a third generation of computing systems to a mass readership.
human/user-oriented claims are probably what makes the AmI vision different from earlier more technology deterministic visions (Punie 2005, p.113).

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. But as more and more activities in daily life, at work and in other environments, will depend on the availability of AmI devices and services in the future, 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.

Most stakeholders acknowledge that there are risks and constraints related to AmI that need to be tackled but little effort has gone, to our knowledge, in investigating what such concrete risks and constraints might be and consequently, in identifying ways to overcome the problematic implications of the dark side of AmI. 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. 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 are realistic future scenarios which highlight threats and vulnerabilities which are subsequently analysed so as to extract useful options aimed at overcoming the identified possible risks.

This paper will argue for the need to have a more realistic approach towards future-oriented technology approaches by painting not only the bright and sunny picture of the potential of new technologies but also their possible grey and even dark sides. It will present such an approach as was developed in the SWAMI ‘dark scenarios’ exercise. It will discuss the conceptual and methodological design of the dark scenarios; will provide some examples from the scenario stories and will give some major outcomes in terms of highlighting threats and vulnerabilities.

---

4 SWAMI stands for Safeguards in a World of Ambient Intelligence; the European Commission FP6 funded project has five partners (Fraunhofer ISI; IPTS – JRC – EC; Vrije Universiteit Brussel; Trilateral Research & Consulting). It stated on February 2005, for 18 months, and aims at identifying a range of safeguards to the threats and vulnerabilities facing privacy, identity, security, trust and digital divide from ambient intelligence. See for all reports and deliverables: http://swami.jrc.es.
2 SWAMI ‘dark scenarios’

2.1 Dark scenarios in Ambient Intelligence

Since its conception, the AmI vision has been taken up and refined by different actors and institutions. A range of scenarios has been developed to depict the different futures of living and working with AmI. Scenarios are considered as one of the main tools for looking at the future, although there are many other prospective methods such as Delphi expert panels. Scenarios are not predictions. Rather, they describe plausible and/or desirable futures and possible ways on how to realise these futures. They can provide provocative glimpses of potential futures and are developed to stimulate the debate on these possible futures. 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 (Gavigan & Scapolo 2001; Godet 2000; Wilkinson 1995). The scenarios developed by SWAMI share these generic goals with other scenario exercises.

The objective of many scenario exercises and foresight studies is to present images of desirable futures and sometimes to determine the necessary steps to realise such futures. Consequently, they have an inherent bias towards presenting only optimistic visions of the future. The SWAMI scenarios are different because they present certain visions of the future that we in principle, do NOT want to become realities. SWAMI has labelled them “dark” scenarios. They depict a realistic future that could emerge from the application of new AmI technologies but focus on the likely adverse effects which often are overlooked by technology developers and policymakers. The first objective of the dark scenario exercise thus consisted of the identification of potential threats and vulnerabilities that need to be mitigated if AmI is to become a future success story.

It is important to emphasise that the SWAMI dark scenarios do not focus on how everything can go wrong with ambient intelligence (See for instance Lucky 1999). They are not anti-technology or neo-luddite, i.e., categorically opposed to technologies in general and to AmI in particular. On the contrary, the SWAMI dark scenarios are intended to be constructive towards realising AmI. Hence the second objective of the dark scenarios that coincides with identifying and proposing safeguards that can address the identified threats and vulnerabilities. These safeguards, as will be shown later, are generic outcomes that can be taken up and further developed by other actors at a later stage. The dark scenario exercise of highlighting vulnerabilities would however not be complete if not followed by an exercise that focussed on safeguards.

The latter approach - identifying hazards and developing safeguards – is similar to approaches followed in the field of risk analysis and risk assessment, as it consists of, broadly speaking, identifying the hazards and assets to be protected, determining the magnitude and likelihood of the occurrence of adverse effects and deciding what precautions need to be made (E.g. Symantec s.d). The difference between the SWAMI dark scenario approach and traditional risk analysis could be that information society kinds of risks seem to be less risky and thus less in need of a structured approach to mitigate them, when compared to the traditional domains of risk analysis: industrial and nuclear hazards, natural disasters, environmental protection and health. These are the domains where the so-called precautionary principle can be applied, as an instrument of risk management when there is scientific uncertainty about the potential dangerous effects on the environment, human, animal or plant health (COM 2000). As a result of seemingly less risky technologies, ICTs are less considered within this frame – except if their impact on health is for instance considered (Hilty et. al 2005), although it could be argued, and this is also an outcome of the SWAMI dark scenario exercise, that AmI risks can be quite
significant as well, especially when societies move towards increased dependence from digital technologies and services based for instance on biometric technologies (E.g. Maghiros et. al 2005) and ICT implants (E.g. European Group on Ethics of Science and New Technologies 2005).

To facilitate identification of these risks but also to provide a complete picture of a future AmI landscape, the SWAMI scenarios assume a wide deployment and availability of ambient intelligence based on the above mentioned ISTAG AmI vision of a future information society where intelligent interfaces enable people and devices to interact with each other and with the environment. It assumes that technology operates in the background while computing capabilities are everywhere, connected and always available. It takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire. It can even engage in intelligent dialogue as it is about human-centred computing, user-friendliness, user empowerment and the support of human interaction.

2.2 Methodology

The SWAMI dark scenarios have been developed in ways similar to other mainstream scenario exercises. The major difference is, as mentioned in the section above, that SWAMI focuses on dark situations, i.e., situations that enable us to highlight vulnerabilities and threats related to AmI; and that safeguards to mitigate the dark situations are considered. As there is no unique method for developing scenarios and as there are different approaches to scenario-writing, it is important to clarify and explain the approach and methodology used by SWAMI.5

The SWAMI scenarios are so-called trend or reference scenarios (Massini & Vasquez 2000). These are extrapolations from current trends. They start from the present and work forward to realistic futures. They do not depict extreme, impossible or unlikely futures.

From the outset, SWAMI decided to develop a number of dark scenarios typical of many scenario exercises, namely four. In principle, a virtually infinite number of possible futures could be developed but it is difficult to manage for both the developers and the readers of the scenarios (Godet 2000; Gavigan et.al. 2001; Wilkinson 1995). Moreover, the design of four scenarios in a scenario exercise makes it possible to plot them on two axes and four quadrants (more details in the next section, see also figure 2).6

The SWAMI scenarios were developed through a combination of desk research and interactive workshops within the consortium and with outside experts in keeping with the view that scenarios should not be based on only desk research (Godet 2000, p.17). More specifically, the SWAMI dark scenarios (or scenarios stories) were constructed as a result of the following activities and associated tools, spread over a period of approximately six months:

5 For an overview of foresight methodologies for the knowledge society, see Miles I., Keenan M, & Kaivo-Oja J., 2003.
6 In the IPTS/ISTAG scenarios on ambient intelligence, for instance, the two axes are efficiency versus sociability and individual versus communal. They contrast applications that serve to optimise efficiency (whether in business or in society) against those that emphasise human relationships, sociability or just having ‘fun’. They also underline the place of ambient intelligence in serving society and the community as well as individuals. See ISTAG, 2001.

THEME: FTA ASSUMPTIONS, METHODS AND APPROACHES IN THE CONTEXT OF ACHIEVING OUTCOMES
<table>
<thead>
<tr>
<th>Activities</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>a state-of-the-art review of projects, studies and scenarios on ambient intelligence, including an investigation of the current legal framework in Europe, as reported in SWAMI Deliverable 1&lt;sup&gt;7&lt;/sup&gt;</td>
<td>- Literature review</td>
</tr>
<tr>
<td>- Collaborative work</td>
<td>- Systematic analysis</td>
</tr>
<tr>
<td>a full-day workshop with 13 external experts to validate the Deliverable 1 review and to brainstorm on the major drivers and axes for developing dark scenarios&lt;sup&gt;8&lt;/sup&gt;</td>
<td>- Validation workshop</td>
</tr>
<tr>
<td>- Experts' interviews</td>
<td>- Brainstorming</td>
</tr>
<tr>
<td>an internal working document summarising the dark scenario brainstorming discussion</td>
<td>- Synthesis work</td>
</tr>
<tr>
<td>an internal two-day consortium meeting to discuss and develop the basics of the scenario scripts and scenario analysis</td>
<td>- Semi-oriented discussion (free discussion on established drivers)</td>
</tr>
<tr>
<td>further development of the scenarios and their analyses via electronic exchanges between the partners</td>
<td>- Iterative loops among partners</td>
</tr>
<tr>
<td>a workshop with 15 external experts to validate the draft report of the scenarios including their analyses and to develop safeguards</td>
<td>- Validation workshop</td>
</tr>
<tr>
<td></td>
<td>- Experts' interviews</td>
</tr>
</tbody>
</table>

The SWAMI partners decided not to create full-blown, extensive scenarios and detailed analyses and descriptions. Rather, we opted for developing four scenarios that highlight potential vulnerabilities and risks in a way that is relatively easy to read and digest.

As a result, the scenario stories are not an end in themselves. This is quite important because often only the scenario scripts receive visibility. SWAMI scenarios however, contain a “technology check”, i.e., references to RTD projects and publications that are, for example, trying to provide solutions to the mentioned problems or that may raise important vulnerabilities. This is also the case for the “reality check”, i.e., the references to recent news reports (especially) of events or situations not so different from those in the scenarios point to the fact that the dark situations are credible and based on reality. As mentioned above, the SWAMI dark scenarios are reference scenarios based on extrapolations from current-day trends. This is quite crucial because too radical or too extreme scenarios would face the risk of being criticised as completely unrealistic and thus maybe even irrelevant. They scenarios are, however, still to be regarded as fictional.<sup>9</sup>

Equally important as the scenario stories is the scenario analysis. SWAMI has developed the following structure for presenting the analysis of each of the four scenarios:

- a short summary of the major dark situations mentioned in the scenario story;
- a list of the most important AmI technologies and/or devices used and/or implied in the scenarios. These are pieces of hardware or software, such as 4G mobile networks that enable applications to be offered;
- a list of major AmI applications that emerge in each scenario. Applications allow certain things to be done with the technologies and devices;

---

<sup>7</sup> Friedewald M., Vildjounaite E. & Wright D. (eds.) 2005.

<sup>8</sup> See for report and minutes of the WP1 Workshop: [http://swami.jrc.es/pages/state_of_art.htm](http://swami.jrc.es/pages/state_of_art.htm). The list of participants is mentioned in the acknowledgments section of this report.

<sup>9</sup> Therefore, all names, persons, companies, organisations, governments, countries, products, devices, places, events, situations and other elements in the SWAMI dark scenarios are purely exemplary and/or fictitious.
• the *drivers* that have led to the scenarios and/or their (dark) situations. Drivers drive or impel a situation or the scenario. An example of a driver is the individual and/or social wish for privacy or security;
• a discussion of the major *issues* in terms of privacy, security, identity and vulnerabilities raised by the scenario, which are the core concerns of the SWAMI project;
• the *legal aspects* implicit in the scenarios;\(^\text{10}\)
• preliminary *conclusions*.

The SWAMI dark scenario approach is summarised in the following graph:

![SWAMI dark scenario approach](image)

**Figure 1: SWAMI dark scenario approach**

In the next section, the choice for the four scenarios developed by SWAMI is explained.

### 2.3 The four scenarios

SWAMI developed four scenarios as follows:

- **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* – takes a different stance, involving a data-aggregating company that becomes victim of theft of the personal data which fuel its core business. Given its dominant position in the market, the company wants to cover this up

---

10 The legal analysis is divided in two parts: a synopsis integrated in the analytical section of each scenario and an extensive legal screening as a separate chapter in the report.

**THEME: FTA ASSUMPTIONS, METHODS AND APPROACHES IN THE CONTEXT OF ACHIEVING OUTCOMES**

- 7 -
but will face the courtroom two years later.
• **Dark scenario 4: Risk society** – suggests AmI as risk society portrayed 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 traffic systems and crowd management in an AmI environment.

The first two scenarios depict the impact of AmI dark situations on the individual and the family in their everyday life. The impact of the AmI dark situations on the individual is at the micro-level. In scenarios 3 and 4, the impact is on a larger societal scale. The theft of personal data in scenario 3 affects millions of people. Scenario 4 also depicts the societal impact of AmI technologies on privacy, the environment and crowd behaviour.

In addition to the individual – societal axis, we have drawn a public – private axis for positioning the scenarios. Both scenarios 1 and 3 deal with private concerns and with what might be called the private sphere. Scenarios 2 and 4 on the other hand encompass concerns situated in the public sphere. Scenario 3 draws out concerns in the transport and health sectors which are regulated by public actors while scenario 4 draws out other public concerns, including those relating to the environment.

The combination of the axes individual/societal and private/public enables each scenario to be placed in a different quadrant.

![Figure 2: Positioning of the four dark scenarios](image)

Thus, as shown in Figure 2, the four scenarios address individual and societal concerns as well as private and public concerns. Nevertheless, the scenarios are constructed from the point of view of the individual citizen, in part to indicate that also societal concerns are experienced by people in their everyday life, be it at work, at home or on holiday or via a TV newscast.

**Theme:** FTA Assumptions, Methods and Approaches in the Context of Achieving Outcomes

- 8 -
Grounding the scenarios in everyday life helps us to reflect upon the use of AmI in situations with which we can identify today and in the future.

2.4 Results of scenario analysis: 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 identified in a consensual way among SWAMI partners and external experts and illustrated by the scenarios in varied situations. These are briefly mentioned below (Friedewald and Wright, eds. 2006):

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.
- **Security**: the scenarios depict security issues in different contexts: security imposed for telework, 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.

**Some examples from the scenarios:**

**Identity issue: People need to take adequate care to protect their cyber identity(-ies)**

Today cyber citizens often use the same password or ID over different websites and systems. The yellow bits of paper 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 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's unlikely to go away. Human nature, being what it is, means that some people just will not take even the most basic of steps towards protecting themselves. From this optic, identity theft may have a salutary effect of being a good learning experience, but this is a bit like saying that walking with your eyes closed across a busy street can be a good learning experience. In any event, once the theft has occurred, it may be as difficult or impossible to recover from as being run over by the number 9 bus.

**Dependency issue: 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 as to whether it is possible to re-establish a previous functional state.
Illustration from Scenario 1:

Paul receives an alarm signal on his Personal Wrist Communicator (PWC). There is an intruder in the house. “How is that possible?” he asks himself. He knows that his son Ricardo is home. He had invited some friends to play a new virtual reality game (for which Ricardo has a licence) from the entertainment centre downstairs. Paul checks the home surveillance system remotely but only gets a still image from 30 minutes ago. There is no live image available from the front and back door cameras, nor is Paul able to play back who has passed in front of the doors today. Ricardo does not answer his calls. “What’s happening? Where is he?”

Victimisation issue

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.

Illustration from Scenario 1:

Paul is just leaving the office to return home when his boss calls, “Come in, Paul. I’m glad you are still at the office. It seems we have a small problem… I’ve just been contacted by the police who have asked for access to all the data we have on you. I understand this is just an informal request so we do not have to give them anything, but, as you know, as a security company, we cannot afford any suspicions of our staff.”

Paul is astonished and does not understand what is happening. First, the home problem, now this. “Surely, this must be some kind of mistake. I don’t know why they’d want my data – although I have heard lately of cases where the police have been investigating innocent people based on inadequate profiling.”

Loss of control issue; malicious attacks and spamming threats: Hijacking 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 the AmI system, they might be able to re-adjust personalised settings and extract sensitive information stored in databases in order to use them illegally.

Illustration from Scenario 1:

---

11 Exactly this situation already occurs today. See, for example, Summers, Deborah, “Bureau admits innocents branded criminals”, The Herald [Scotland], 22 May 2006: “The Home Office was plunged into yet more controversy yesterday as it emerged nearly 1500 innocent people had been branded criminals because of errors by its Criminal Records Bureau.” http://www.theherald.co.uk/politics/62460.html
Paul receives multiple messages on his PWC the moment he leaves his boss’s office. He had all incoming communications on hold from the moment he entered her office. This is a company default setting. There is one message that immediately attracts his attention. “If you want your house systems to work again, click on the following link...” “What? I’m being blackmailed! So that’s why I couldn’t get access to my home systems, nor could the local security agent. That’s why I got the intruder message,” he thinks, slightly reassured, since that probably means that his children at home are OK.

3 Main conclusions

3.1 Developing safeguards

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 3 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.

3.2 Methodological issues

The SWAMI dark scenarios have been developed in ways similar to other mainstream scenario exercises. This means for instance that the scenarios were developed through an iterative process of desk research, group discussions and interactive workshops. It also entails that SWAMI has reduced the number of possible scenarios to four dark scenarios encompassing both individual and societal concerns, on the one hand, and private and public concerns, on the other hand.

The scenario stories are not an end in themselves. SWAMI has emphasised that the prospective exercise was not just about writing appealing scenario stories or scripts by way of developing a consistent analytical framework that accompanies each of the four scenarios. This framework comprises the following elements:

- the major dark situations mentioned in each scenario story;
- the most important AmI technologies and/or devices used and/or implied in the scenarios;
- the major AmI applications referenced in each scenario;
- the major drivers that have led to the scenarios and/or their (dark) situations;
- a discussion of the major issues in terms of privacy, security, identity and vulnerabilities as these are the core concerns of the SWAMI project;
- the legal aspects involved when things start to go wrong with AmI;
- preliminary conclusions.

Moreover, the scenario stories were checked to see if the stories made sense from both a technological point of view (“technology check”) and a realistic point of view (“reality check”), since the SWAMI dark scenarios are reference scenarios based on extrapolations from current-day trends. Hence, although the scenario stories themselves are fictions, they are based on reality. This is quite important because extreme and unrealistic scenarios might be dismissed as being irrelevant. That would also undermine the consequent activity of developing safeguards.

The SWAMI dark scenario exercise is different from most scenario exercises, to our knowledge, because if its focus on dark situations, on identifying threats and vulnerabilities based on these dark situations and, not the least, because of the development of safeguards to mitigate these risks. Especially the latter shows that the SWAMI dark scenarios are a constructive undertaking towards realising a safe and secure AmI. It was not the objective to be negative about the potential of AmI but rather on the contrary, to contribute to making AmI a future success.
3.3 Final remarks

The SWAMI dark scenario exercise was quite a delicate exercise as it needed to strike an acceptable balance between the threats and vulnerabilities of future AmI landscape in Europe on the one hand, and its potentials and strengths on the other hand. The scenarios could certainly not be too negative. With the advantage of hindsight, it could even be argued that the use of the term dark was maybe not fully appropriate. Some would argue that the scenarios are more grey than dark. Others would contrast them with bright scenarios. But as the scenarios encompass both potentials and risks of future IST technologies, maybe they are just "realistic", as life is never fully black or white either and a zero risk society is impossible and probably also undesirable. This would mean that a scenario approach for future-oriented technology analysis (FTA) would need to encompass threats, vulnerabilities and safeguards together with the strengths and opportunities of new technologies.

REFERENCES:


THEME: FTA ASSUMPTIONS, METHODS AND APPROACHES IN THE CONTEXT OF ACHIEVING OUTCOMES

- 15 -

