Safeguards in a World of Ambient Intelligence (SWAMI)

Deliverable D2

Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities

January 2006

Editors: Yves Punie, Sabine Delaitre, Ioannis Maghiros & David Wright

Authors: Petteri Alahuhta, Paul De Hert, Sabine Delaitre, Michael Friedewald, Serge Gutwirth, Ralf Lindner, Ioannis Maghiros, Anna Moscibroda, Yves Punie, Wim Schreurs, Michiel Verlinden, Elena Vildjiounaite, David Wright

Final version

Project Co-ordinator:	Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research, Breslauer Straße, 76139 Karlsruhe, Germany, E-Mail: m.friedewald @ isi.fraunhofer.de
Partners:	Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany. Contact: Michael Friedewald. http://www.isi.fraunhofer.de
	Technical Research Center of Finland, VTT Electronics, Oulu, Finland. Contact: Petteri Alahuhta (Petteri.Alahuhta @ vtt.fi). http://www.vtt.fi/ele/indexe.htm
	European Commission/Joint Research Center-Institute for Prospective Technological Studies, Seville, Spain. Contact: Ioannis Maghiros (ioannis.maghiros @ cec.eu.int). http://www.jrc.es
	Free University Brussel, Center for Law, Science, Technology and Society Studies, Belgium. Contact: Serge Gutwirth (serge.gutwirth @ vub.ac.be). http://www.vub.ac.be/LSTS/
	Trilateral Research & Consulting, London, United Kingdom. Contact: David Wright (david.wright @ trilateralresearch.com). http://www.trilateralresearch.com/
Project web site:	http://swami.jrc.es

We suggest the following citation format: Punie, Y., Delaitre, S., Maghiros, I. & Wright, D. (eds.) "Dark scenarios on ambient intelligence: Highlighting risks and vulnerabilities". SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission under contract 006507, November 2005. http://swami.jrc.es

ACKNOWLEDGEMENTS

SWAMI would like to thank the following experts for their participation in the SWAMI Work Package 1 Workshop, June 1, Brussels, 2005.

Laurent Beslay, European Data Protection Supervisor, Brussels, Belgium;

Ian Brown, Foundation for Information Policy Research, London, United Kingdom;

Markus Hansen, Independent Data Protection Centre Schleswig-Holstein, Kiel, Germany;

Mario Hoffmann, Fraunhofer SIT, Darmstadt, Germany;

Pertti Huuskonen, Nokia Research Centre, Tampere, Finland;

Achilles Kameas, Research Academic Computer Technology Institute, Patras, Greece;

Spyros Lalis, University of Thessaly, Greece;

Miriam Lips, Tilburg University, Netherlands;

Irene Lopez de Vallejo, University College London, United Kingdom;

Gregory Neven, KU Leuven, Belgium;

Albrecht Schmidt, University Munich, Germany;

Stefaan Seys, KU Leuven, Belgium;

Michael Vanfleteren, KU Leuven, Belgium.

Disclaimer
The content and orientations of this report should not be taken as indicating a position of the people mentioned above. The responsibility for the report lies fully with the authors and editors.

Contents

Acknowledgements

EXECUTIVE SUMMARY

PURPOSE OF THIS REPORT

A driver of all ambient intelligence (AmI) technologies is the extended personalisation of services required by virtual communities sharing common interests whether in the private or public domain. Our technological environment is transformed as elaborate e-services develop and individuals massively adopt them. The existing human-machine interface, which is made more complex through the introduction of virtual identities, is no longer intuitively understood nor is its control easy to manage. It was hoped that the intelligent environment would allow the effortless administration of the apparent complexity but we now understand that this will not happen and that in essence the environment is not really intelligent (the way people define intelligence) but it only appears intelligent when judged from the outside.

Multiple threats may well arise as a result of yet unidentified vulnerabilities in the AmI systems and in turn may lead to our loss of control over and trust in the technological environment that surrounds us and those who drive it. Moreover, the situation is aggravated as "big" and "little" "brothers"[1] impose diverse agendas. A likely solution should be democratically established, balanced in terms of security and protective of privacy. SWAMI – Safeguards in a World of Ambient Intelligence – is a multidisciplinary research project on the social, legal, organisational and ethical issues associated with ambient intelligence, which places the individual at the centre of future developments for an inclusive knowledge-based society. The project is investigating the emerging challenges, in particular with respect to privacy, security, identity, trust and protection of rights for all citizens in all their roles (private and professional) in the Information Society. SWAMI aims at identifying threats and system vulnerabilities and appropriate safeguards by developing and analysing future scenarios, more precisely "dark scenarios", in order to analyse and understand future risks and vulnerabilities related to ambient intelligence.

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. Most scenarios are developed so as to demonstrate the benefits of new technologies. SWAMI scenarios are "dark" since they include applications that go wrong or do not work as expected.

The main purpose of this deliverable has been to develop "dark scenarios" which highlight the potential risks, vulnerabilities and policy implications in the deployment of ambient intelligence technologies so as to put the emphasis on the need to develop safeguards and protections to minimise the risks that could emerge in this new intelligent environment. As a result, we view the SWAMI dark scenarios as a

[1] The Orwellian vision of "big brother" was that the state had the power and technology to engage in surveillance, but with decreasing size and price, surveillance technologies have become "democratised". Today, new threats come from the little brothers, companies, neighbours, even relatives. See Rheingold, H., 2003.

constructive undertaking towards realising a safe and secure AmI.

MAJOR CONCLUSIONS

Many messages have been established from the analytical and legal treatment of 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.

Key SWAMI issues

- **Privacy**: it is important to be aware of the implications of AmI on private life and personal data and to take adequate social, technical, economic and legal measures to protect 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**: security is a key challenge for successful AmI implementation. 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. The possible impacts that arise when there is a lack of security or unsuitable security measures are also underlined.
- **Identity**: the different components of identity, i.e., information related to legal identity, identification, authentication and preferences, play important roles in determining the feasibility of the AmI environment. The scenarios expose and detail the consequences when identity-based data are misused, erroneously used or incompletely processed.
- **Trust**: the notion of trust has technical aspects as well as social, cultural and legal aspects. In the scenarios, trust is raised in different connections: trust and confidence, lack of trust (from loss of control, unwillingness to provide some data, contextual misunderstandings) and honesty.
- **Loss of control**: it is one of the main issues in the SWAMI dark scenarios and 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. It can also emerge when the complexity level of AmI devices or services is too high and consequently does not enable users to get what they want. Strategies should be defined in order to compensate for the complexity and to weaken this feeling of loss of control.
- **Dependency**: this issue directly emerges from the usage of a technology by the user and the prospects (benefits and alternative solutions) of the technology. The scenarios mainly highlight its social impacts. Several situations are described, 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): exclusion may be voluntary, for instance, when a user switches off, but usually it is outside people's own will. 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. Exclusion can also be the

result of lack of interoperability, denial of service, inadequate profiling and data mismatches.

- **Victimisation**: Citizens have a democratic right not to be treated as criminals (unless they are criminals, of course), otherwise, they will be unfairly victimised. 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) and without being subject to anonymity profiling.

Dark scenarios and threats

- **Surveillance**: every citizen/consumer leaves electronic traces as the price of participation in the ambient intelligence society. These traces enable new and more comprehensive surveillance of our physical movements, use of electronic services and communication behaviour. 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 give malicious persons many opportunities to steal identity information and to use it for criminal purposes. SWAMI dark scenarios give a picture of identity theft in AmI space. And a new kind of crime regarded as a subsequent act of identity theft is raised; it is the case of data laundering.
- **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. Not only is the technical dimension of this threat described but also its social and organisational dimensions in AmI space. It shows that ambient intelligence services are not automatically becoming public utilities at the service and benefit of all. It is not self-evident that AmI services will become as widespread as mobile communications, especially in developing countries.
- **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.

THE SWAMI SCENARIO APPROACH

The deliverable first describes the methodology that was developed and used by SWAMI for the scenario exercise and then the different scenarios which are the basis of a broader reflection on the major issues and threats. A legal analysis follows and then conclusions are provided which will eventually lead to determining safeguards.

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.

Four dark scenarios have been elaborated that encompass both individual and societal concerns, on the one hand, and private and public concerns, on the other hand. These two scenario axes (individual-societal and private-public) have helped reduce the virtually infinite number of possible futures that could be developed to a manageable number of 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 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 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 two years later. The scenario draws attention to the digital divide between developed countries with 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.

The report contains a special chapter providing a detailed legal screening of the scenarios. This is done according to the following analytical structure for each situation identified as relevant: a *Scenario description* presents in brief the facts upon which the analysis is based; a *Scenario link* contains a quote from the scenario script to indicate the position or significance of the situation in the scenario; a *Legal field* mentions which legal fields could apply to the situation; a *Legal chapter* refers to the specific chapter of the legal text; a *Discussion* is the section where the legal issues and problem areas are developed; and a *Conclusion* contains a short statement on the issue.

This report is the second deliverable of SWAMI for the development of safeguards for a world of ambient intelligence. The SWAMI project will next specify the vulnerabilities discussed and validated in the light of the interest of various AmI constituencies. The identified opportunities and risks will be contrasted and balanced to each of the affected user groups and applications. Moreover, we will consider how and to what extent it is possible to overcome the problematic implications of the dark side of ambient intelligence through the use of various safeguards and privacy-enhancing mechanisms

(PEMs). The final objective is to ensure user control and enforceability of policy in an accessible manner and the protection of rights for all citizens in all their roles (private and professional) in the Information Society.

1 INTRODUCTION

1.1 THE SWAMI PROJECT

SWAMI (Safeguards in a World of Ambient Intelligence) is a project funded by the European Commission under the Information Society Programme (IST) of the Sixth Framework Programme (FP6). It looks at the challenges and bottlenecks facing the realisation of the vision of ambient intelligence as the next stage of the information society in Europe.

While most stakeholders paint the promise of ambient intelligence (AmI) in sunny colours, there is a dark side to AmI as well. In a way, this dark side is inherent in many technologies including AmI, where intelligence is embedded in the environment and accessible anywhere and at any time including by those on the move. In this future, virtually every product and service – our clothes, money, appliances, the paint on our walls, the carpets on our floors, our cars, everything – will be embedded with intelligence. With networking microchips tinier than a pinhead, personalised services can be provided on a scale dwarfing anything hitherto available. That being the case, there will be a lot more personal information stored somewhere, far more than in today's world. Moreover, many more activities in daily life, at work and in other environments, will depend on the availability of AmI devices and services. The risks involved in such an endeavour are great and need to be mitigated. These issues lie at heart of the SWAMI project.

SWAMI has three major tasks:

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

SWAMI (http://swami.jrc.es) also intends to contribute to integrating and structuring the European Research Area mainly by generating awareness within the AmI community of the security, privacy, identity, accessibility and other issues that should be taken into account in the formulation and implementation of AmI projects and by providing the footing for related issues to be addressed in projects funded under the Seventh Framework Programme.

There is an urgent need for realising these objectives. Matters of identity, privacy,

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

1.2 DARK SCENARIOS IN AMBIENT INTELLIGENCE

Ambient intelligence is a key to the future information society. It is based on the development of current and next-generation IST technologies and promoted by, amongst others, EU policy-makers. AmI is a priority within the FP6 IST programme for the period 2002-2006 as well as other pan-European and national research programmes. This 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.[2]

IST applications and services must be trustworthy, secure and reliable, as stated in the recent i2010 plan from the European Commission.[3] The plan also confirms the strategic importance for the development of the information society of the themes dealt with by SWAMI such as interoperability, security and reliability, identity management, rights management and ease of use, including the importance of raising awareness of the need for self-protection, vigilance and monitoring of threats, rapid and effective response to attacks and system failures.

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.[4]

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 visions of the future that, as stated earlier, we do NOT want to become realities. SWAMI has labelled them "dark" scenarios. The SWAMI scenarios do not focus on how everything can go wrong with

[2] European Commission, 2002, pp. 4-6.
[3] COM(2005) 229 final
[4] Gavigan & Scapolo 2001; Godet 2000; Wilkinson 1995.

ambient intelligence.[5] They rather depict an undesired but realistic future that could emerge from the application of new AmI technologies. From a methodological point of view, the SWAMI scenarios are so-called trend or reference scenarios.[6] 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. 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. Their objective is to highlight potential vulnerabilities and risks that need to be mitigated if AmI is to become a future success story.

1.3 THE SWAMI DARK SCENARIOS

1.3.1 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. 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.[7]

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.[8] Moreover, the design of four scenarios in a scenario exercise makes it possible to plot them on two axes and four quadrants.[9]

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.[10] More specifically, the SWAMI dark scenarios were constructed as a result of the following activities:

- 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;[11]
- a full-day workshop (1 June 2005) with 13 external experts to validate the Deliverable 1 review and to brainstorm on the major drivers and axes for developing dark scenarios;[12]

[5] See, for instance, Lucky, R. W., 1999.
[6] Massini & Vasquez, 2002.
[7] For an overview of foresight methodologies for the knowledge society, see Miles I., Keenan M, & Kaivo-Oja J., 2003.
[8] Godet, 2000; Gavigan et.al., 2001; Wilkinson, s.d.
[9] 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.
[10] Godet, M., 2000, p.17.
[11] Friedewald, M., Vildjiounaite, E. & Wright, D., 2005.
[12] See WP1 Workshop minutes including the agenda on the SWAMI website:

- an internal working document summarising the dark scenario brainstorming discussion;
- an internal two-day consortium meeting (28-29 June 2005) to discuss and develop the basics of the scenario scripts and scenario analysis;
- further development of the scenarios and their analyses via electronic exchanges between the partners;
- a workshop with 15 external experts to validate the draft report of the scenarios including their analyses and to develop safeguards (29 November 2005).

The SWAMI scenarios assume a wide deployment and availability of ambient intelligence based on the ISTAG AmI vision of a future information society where intelligent interfaces enable people and devices to interact with each other and with the environment. Technology operates in the background while computing capabilities are everywhere, connected and always available. AmI is based on the convergence of ubiquitous computing, ubiquitous communication and intelligent, user-friendly interfaces. This intelligent environment is aware of human presence and preferences, takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire. It can even engage in intelligent dialogue. It is about "human-centred computing", user-friendliness, user empowerment and the support of human interaction.[13]

The SWAMI partners decided not to created 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. SWAMI scenarios 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. They are, however, still to be regarded as fictional.[14]

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;
- the *drivers* that have led to the scenarios and/or their (dark) situations. Drivers drive

---

http://swami.jrc.es/pages/state_of_art.htm. The list of participants are mentioned in the acknowledgments section of this report.

[13] See ISTAG, 2001 and subsequent ISTAG documents at www.cordis.lu/ist/istag.htm; Harwig & Schuurmans, 2002. For a review of the vision, see Punie, 2005.

[14] Therefore, all names, persons, companies, organisations, governments, countries, products, devices, places, events, situations and other elements in the SWAMI dark scenarios are purely exemplatif and/or fictitious.

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;[15]
- preliminary *conclusions*.

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

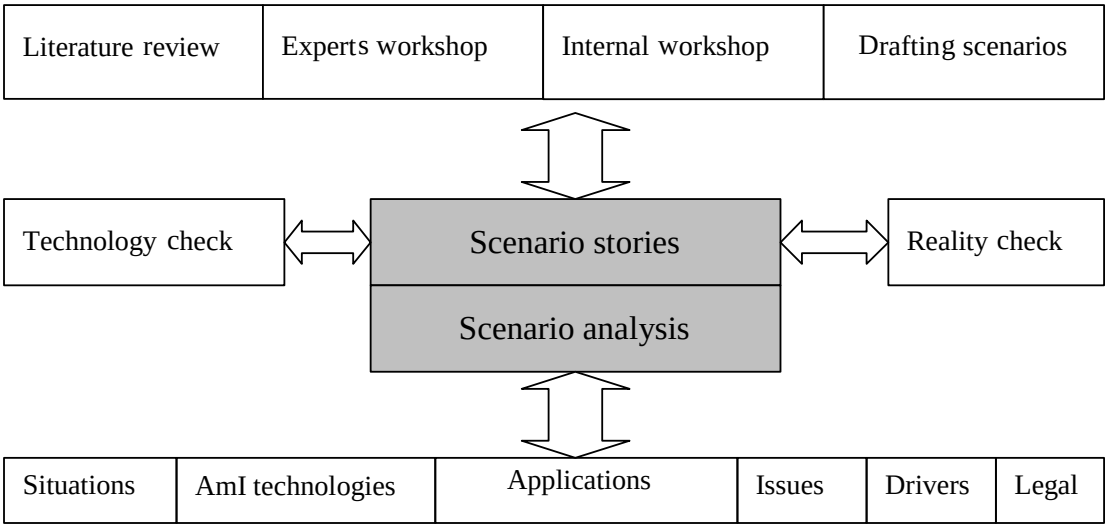

Figure 1: SWAMI dark scenario approach

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

1.3.2 Drivers and issues

The choice to develop certain scenarios and not others is based on the methodology mentioned above. It is certainly not arbitrary. Scenario workshops were used to identify the most important drivers that gave rise to the kind of scenarios being developed and to identify the most important issues that needed to be present in the scenarios. During the experts workshop organised by SWAMI, two sessions were organised to prepare for the dark scenarios. They consisted of a "post-it" session to identify the major drivers and/or issues that needed to be taken into account when developing dark scenarios and a session that focussed on the clustering and prioritisation of these drivers/issues. Since the objective of the exercise was to have a broad orientation for the scenarios, drivers and issues were treated together even though, strictly speaking, they are not the same.

The table below presents the result of the exercise. It also contains a prioritisation. The 10 clusters were ranked by the participants according to impact and certainty. Drivers/issues that are expected to have a major impact got five points against one point for little impact. Also, the degree of certainty that these drivers will have an effect was

[15] 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.

ranked according to five (high certainty) and one (low certainty). The average of both was multiplied to get an assessment score that indicates the importance of the driver/issue, with lowest being between one and five and highest between 20 and 25.

Position	Top 10 issues/drivers	Impact average[16]	Certainty average	Impact x certainty
1	Loss of control	4.53	4.26	19.30
2	Increased possibilities for surveillance	4.16	4.21	17.51
3	Profiling	3.79	4.42	16.75
4	Risk – trust - crime opportunities	3.47	4.16	14.44
5	Complexity (value)	3.47	4.05	14.08
6	Individual transparent, power opaque	3.89	3.53	13.73
7	Dependence	3.37	3.63	12.23
8	Non-participatory (process)	3.32	3.37	11.17
9	Exclusion	3.32	3.26	10.82
10	Costs	2.84	3.63	10.32

Table 1: Top 10 issues/drivers

The issues regarded as most important both in terms of impact and certainty were fear of loss of control, the increased possibility for surveillance offered by AmI, profiling, and security risks, and new opportunities for crime. Complexity encapsulates many things but here mainly relates to the difficulty users have in understanding the decision-making process behind intelligent systems and the way value (i.e., valuable information) is produced.

Other concerns relate to the "death of privacy" in a future where individuals are completely transparent in contrast to power structures that tend to be opaque, dependency on AmI systems, minimal participation by citizens and consumers in the process of developing and implementing AmI systems, and the risks that certain groups of people will be excluded from our AmI future. Cost was also raised as both an enabler and a bottleneck for AmI.

These issues are recurrent themes throughout this report. They can be seen

- from an individual perspective, where individuals feel they are not in control of the technologies, rather that they are being controlled by the technologies, and
- from a societal perspective, where there is a gap between those groups with the resources to combat a loss of control over technologies and those without the intellectual, social or financial resources needed to avoid exclusion from having a choice to use and benefit from the technologies.

The individual – society pair forms one axis for the positioning of the four dark scenarios, as presented in the next section.

[16] Total score divided by numbers of votes cast. Nineteen votes were cast.

1.3.3 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 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/or 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.

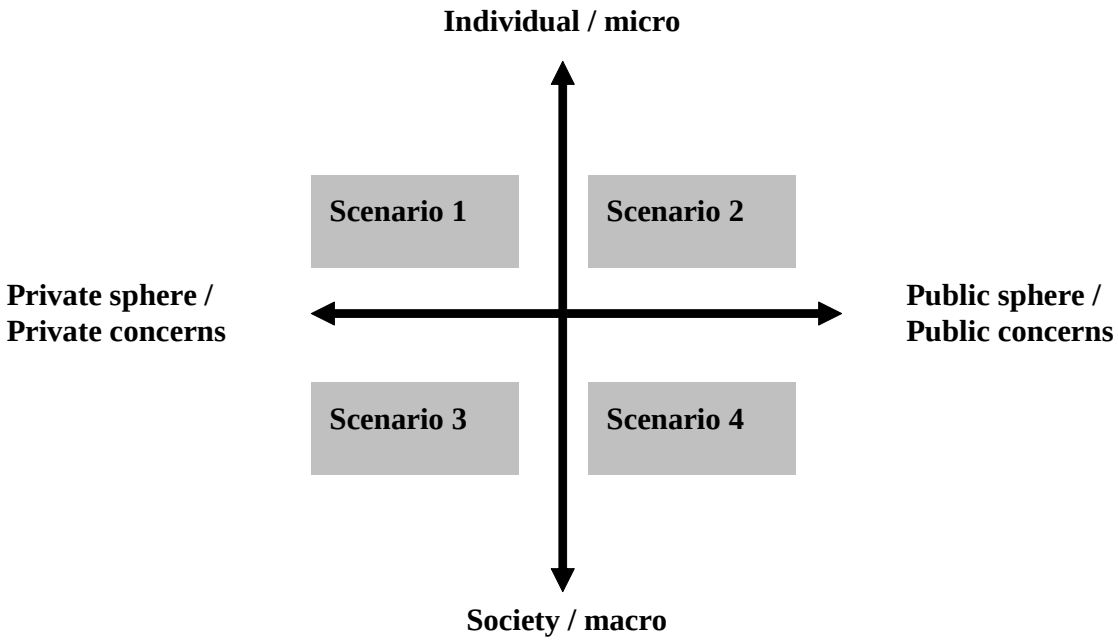

Figure 2: Positioning of the four dark scenarios

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. 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.

1.4 STRUCTURE OF THE REPORT

Chapter 1 of this report introduces the SWAMI project and the dark scenario approach and methodology. Chapters 2 to 5 contain the four dark scenarios. Each scenario chapters consists of three major sections: the scenario script, the scenario analysis and some conclusions. A detailed legal screening of the scenarios is provided in chapter 6. The next chapter concludes the report by presenting the major issues that will be taken up in the forthcoming work of SWAMI on safeguards and policy options. Section 8 gathers all the references used in this report.

2 DARK SCENARIO 1: A TYPICAL FAMILY IN DIFFERENT ENVIRONMENTS

2.1 THE SCENARIO SCRIPT

Scene 1: At home and at work

The Sebastianis are a middle-class income family who make intensive use of their smart AmI home. Both parents work full-time but with flexible hours. The father (Paul) mainly works from home for a private security company. His work concerns remote surveillance of company premises. His wife Maruja works for a real-estate company in the city. They have two teenage children (Ricardo and Elena).

Importance of face-to-face contacts, also in an AmI world	*Paul has been called out for a meeting at the security company. Such meetings where security agents have face-to-face contacts are organised only occasionally. Although he likes working from home, Paul also enjoys actually meeting the colleagues with whom he collaborates on a daily basis.*
Security imposed for tele-work *AmI addresses results of forgetting*	*He forgot to close the door of his highly protected study when he left the house. Usually, this is not a problem. The room knows when Paul leaves because embedded sensors in the room detect inactivity.*[17] *Unfortunately, the door with fingerprint reader was not closed automatically because a carpet was misplaced and folded accidentally. It prevented the door from closing.*
Personal Wrist Communicator (PWC) *DRM: licence fee connected to IP number*[18] *Feeling of loss of control: "What is going on?"*	*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?"*
Physical check *On the spot back-up*	*Paul contacts the neighbourhood security service and asks them to check visually on his house and children. From the outside, nothing seems to be wrong except that all curtains and windows are closed. Moreover, it seems that all security*

[17] Embedded Everywhere: A Research Agenda for Networked Systems of Embedded Computers, http://books.nap.edu/html/embedded_everywhere/

[18] "Green light to chase file-sharers", *The Local*, 13 October 2005. http://www.thelocal.se/article.php?ID=2282&date=20051013

access to security system *False alarm(burden on system operation)*	*systems are blocked and the security agents on the spot cannot get access to the security surveillance logs. Paul is informed of the situation and decides to call the police. In the past, AmI security systems alarmed the police automatically but because of too many false alarms, this procedure has been stopped.*
Disproportionate reaction on suspicion	*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."*
Inadequate profiling on 35% match only	*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."*[19]
Trust and confidence	*"Yes, I know, Paul," she says. "And I trust you, but you must understand that under such circumstances, I can't go to the board of directors meeting tomorrow with a proposal for your promotion at a time when you are being investigated by the police. I'm sorry, but we'll just have to wait until this situation is clarified."*
Unpleasant consequences of unfounded suspicions	*"Okay, sure, I understand," Paul replies. He is disappointed to miss a promotion now, but he is confident that the opportunity will come around again. "I really don't know what the police could be after, but, of course, the best thing to do is to co-operate and let's clear up this misunderstanding." This is what he says, but what he thinks is "This is not my best day, but first I need to find out what's happening at home."*
AmI and priorities of incoming communications	*Paul receives multiple messages on his PWC the moment he leaves his boss's office.*[20] *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…"*
Digital blackmail	*"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*

[19] Singel, Ryan, "Nun Terrorized by Terror Watch", *Wired News*, 26 September 2005. http://www.wired.com/news/privacy/0,1848,68973,00.html

[20] Alahuhta, P., Jurvansuu, M. & Pentikäinen, H., 2004

are OK.

Human security weakness

Biometrics spoof

ID theft within the family (not malicious)

Little brother (privacy breach)

Automated payments make it easy to spend money

Ricardo is indeed enjoying himself with his friends in Paul's study. They were able to enter because the door was still open. At last, he has the opportunity to check whether the print-out he has of his father's iris can fool the iris scanner which it must do, if Ricardo is to unlock his father's computer. It does because Paul still has an old-fashioned model without liveness testing![21] With his father's profile and identity, Ricardo can circumvent the parental control system that governs use of the Internet by all terminals in the home. It's time for some fun. Ricardo places a bet on a sports gambling site, downloads some xxx-rated movies and games on his personal space on the family server and checks out his father's online favourites.[22] "Hmmm, I didn't know the old man likes erotic poetry. And I see he's just bought some pretty pricey lingerie… Well, I hope it's for mum," Ricardo laughs. But he won't be laughing when his father finds out that Ricardo has spent 200 euros from his account.

Human security weakness: easy to guess passwords

While one of his friends goes to the entertainment room to start a multi-player virtual reality game, Ricardo goes to the kitchen to prepare some gin-and-tonics. The cupboard containing the alcohol can only be opened by a numerical code, but Ricardo figured that out long ago. The code is the date of his parents' wedding anniversary.[23]

Scene 2: Shopping while being at work

Shopping Assistant Software (SAS)

Circumventing parental control

Across town, Paul's wife Maruja needs to find a funny (farewell to girlhood!) present for her best friend. Because she is busy at work, she decides to try her new Shopping Assistant Software (SAS) which, according to the hype, is supposed to have intelligent search capabilities and an advanced speech interface.[24] But Maruja is not impressed. The SAS's suggestions seem too ordinary, so she instructs the SAS to keep searching "until you find something really funny."[25] On her way back to the office, Maruja notices that she has received a message from her daughter Elena on her Personal Wrist Communicator (PWC) for a special offer on the new "Real Magic Experience" (RME) she wants for her next birthday. Elena knows her mother would never buy her such an expensive game but with

[21] Daugman, J., 2005 ; Maghiros, I., Punie, Y., Delaitre, S. et al. 2005.
[22] A recent study indicates that spyware risks are highest for broadband users and for those who visit pornographic sites or play games online: http://news.bbc.co.uk/1/hi/technology/4659145.stm
[23] Not everything in the smart house is accessed via biometric verification. But then, the human tendency to use easy-to-guess passwords and/or access codes continues to constitute a possible security weakness. For more on the security weakness of passwords, see Schneier, 2004.
[24] Garate, A., Lucas, I., Herrasti, N. & Lopze, A., 2004.
[25] Dey, A. & Mankoff, J., 2005.

	in view of a really good online offer, she might. The snag is that the offer is only valid for one hour. What Maruja does not know is that this new version of RME will allow Elena to play it at school without the teacher's noticing it.
Privacy preferences *Data laundering*	*Neither Maruja nor Elena is aware that the website with the attractive offer contains a powerful spyware program that looks for personal data and preferences, so that users can be targeted with personalised advertising. The spyware helps to reveal a person's attitude towards privacy and spam.*[26] *Companies are paying a lot of money for personal and group profiles.*[27] *This phenomenon is known as "data laundering". Similar to money laundering, data laundering aims to make illegally obtained personal data look as if they were obtained legally, so that they can be used to target customers.*
Decision taken in a hurry	*Maruja receives the message from her daughter just before a business meeting starts. She looks at the message in a hurry and, attracted by the discount price, she buys the game. Turning her thoughts to the meeting, she is confident she will be able to convince her prospective client, a construction company, to invest in the land held by her company. If she's right, she expects a big annual bonus.*
Embarrassment *Accidental mistake*	*While giving her presentation, Maruja receives, much to her surprise, because she thought she had banned incoming messages, a "Most Funny Wedding Present" advertisement. She accidentally activates the message and displays it on the big screen. It shows an ad for a sex-related product. Flustered and embarrassed, Maruja apologises and continues with her presentation, but she never really gets back on track after that.*
Monitoring *Looses bonus on the basis of incorrect information*	*An audio track of the meeting is recorded and converted to a document, as is normal practice in Maruja's company (thanks to AmI, nobody needs to write and distribute "meeting minutes" anymore!). Next day, Maruja's boss, surprised by the partners' decision to postpone financing of a joint project, checks the meeting report and gets the impression that Maruja did not prepare her presentation well enough. She will probably not get the annual bonus she was counting on. The reason for Maruja's embarrassment was not recorded to the "meeting minutes" since it was a video message, not an audio advertisement.*

[26] Krebs, Brian, "Hacked Home PCs Fueling Rapid Growth in Online Fraud", *Washington Post*, 19 September 19 2005.
http://www.washingtonpost.com/wp-dyn/content/article/2005/09/19/AR2005091900026.html

[27] Vijayan, Jaikumar, "ID Theft Continues to Increase. More than 13 million Americans have been victimized, new study reveals", *Computerworld*, 30 July 2003.
http://www.pcworld.com/news/article/0,aid,111832,00.asp
Zetter, Kim, "TSA Data Dump Leads to Lawsuit", *Wired News*, 14 July 2005. http://www.wired.com/news/privacy/0,1848,68560,00.html

Scene 3: At the park

Location-based advertising and spam *Smart clothes/screen* *Suggestions based on personal profile*	*After the terrible business meeting experience she has had, Maruja leaves the office for a lunch break. She decides to buy a take-away sandwich and walks towards the park. She is receiving almost continuously messages on the flexible screen on her sleeve.[28] She likes the blouse she borrowed from her friend to test the on-screen possibilities of this smart piece of clothing. The screen shows there is a tai-chi gathering on the east side of the park. She might want to join because of her interest in relaxation exercises and in Eastern philosophies.*
User needs to feed AmI with info. If not, avatar mistakes cause annoyance *Irritation*	*"Not today," she thinks, "and I am certainly not having lunch in the Chinese restaurant around the corner, despite its interesting price. I do not like Chinese food. My avatar should know that and I already have a sandwich… Damn, I should have indicated that I already had lunch. You have to think of everything here." The avatar could not know that she already has a sandwich, because she paid cash for it.*
Annoyance leads to switching off	*Another ad appears: "Special offers from the bookshop next door." Maruja gets annoyed by the location-based spam[29] and decides to switch off almost completely, only allowing incoming 'emergency' messages.*
Dependence on AmI filtering *Missing opportunities* *AmI disfavouring personal contacts (exclusion)*	*Later, she finds out that her boss has phoned twice. She also missed a proximity message that a good friend was sitting in a nearby pub. She feels deprived and angry because it is so difficult to get the thresholds of her avatar right. It seems there will always be grey zones where intelligent agents are not able to take the most intelligent filtering decisions. "I should have been more open to the physical environment," she thinks, because then she would probably have noticed that she had passed one of her friend's favourite bars.*
Early adopter	*Maruja thinks about her friend Claire who is always fast in adopting new electronic gadgets such as this blouse. Maruja likes it. It seems really practical.*
AmI facilitated crime	*Claire, however, at that moment, is having a rather bad experience. She is working at home when burglars break into her apartment. The burglars are surprised to find Claire at home. In the ensuing confrontation, Claire is punched in the face. The burglars get away with only her PWC, her wallet and some jewels that were lying on the table but the experience of*

[28] Espiner, T., "Philips unfurls prototype flexible display". http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39216111,00.htm

[29] Paciga, M. & Lutfiya, H., 2005.

Storage of profiles Unlucky coincidence of circumstances

getting robbed will haunt Claire for a much longer time. Moreover, she will now have to train her new PWC from scratch because she did not want to store her profile online, and because the burglars have destroyed her home computer which Claire had used to back up her PWC.

Theft, crime, mixing-up of IDs, wrong identification

The burglary and mugging occurred because of an unlucky coincidence of circumstances, i.e., that Maruja was wearing Claire's blouse when she went to the park where the criminal gang happened to be operating. As she was passing by, the gang "read" the RFID tag embedded in the blouse. As a result, the gang found out that the blouse had been sold at a certain shop. The gang hacked the client database to discover Claire's profile (a well-off woman living alone in the richer part of the city).[30] On the assumption that Claire was wearing the blouse, the criminals decided to break into the apartment and to steal whatever luxury goods they could find.

Not being able to use AmI

After passing by the gang, Maruja is stopped by a young foreign woman. "Excuse me," she asks, "I want to go to the town hall in the central market square. Can you tell me which exit from the park to take?"

"Sure, lets look it up." Maruja clicks on the city map that locates their position and in the blink of an eye; they find that is the right exit on upper-east side. "Thank you," the young woman replies and walks on.

Maruja wonders why this woman does not have her own location device. She would feel completely lost without hers.

Still possible to forget (to authorise)

New forms of crime exploiting weaknesses in imperfect information networks

The location device is not perfect, as Maruja knows from her experience last week when some thugs forced her to hand over her "smart" purse which did not require any authentication in order to make small payments. Maruja had forgotten to authorise an update of the location-based software and found herself walking in an area of the city frequented by drug addicts and criminals. Because there are so many surveillance cameras everywhere these days, criminal gangs and other bad sorts now move quickly from one area to another, taking advantage of the fact that the security information system only gets updated every month and that only subscribers receive these updates.

[30] Knospe, H., Pohl, H., 2004.

2.2 ANALYSIS

2.2.1 Situations

Scenario 1 presents three different environments to depict AmI-related privacy and security weaknesses: at home, at work and in an open public space. There are differences between these environments but the distinction between them is blurring. Already today, ICTs enable work to be brought home and contact with the home at work. This trend will continue with AmI, although it can lead to some problems as shown in the scenario.

Scene 1: At home and at work

The scenario starts with a situation that shows that although many people could be tele-working in the future, face-to-face contacts are still important. Ricardo is able to make use of the father's absence to enter the study before the smart room closes the door. Paul's employer has imposed certain security measures to enable Paul to work at home. One of these is the fingerprint scan needed to open the study door. Another is the biometric protection via iris recognition but Ricardo is able to spoof that with a picture of Paul's iris because the iris scanner is cheap and of low quality. Then, Ricardo is able to use his father's identity to bypass the parental control system and to shop online. Another security weakness is the easy-to-guess passwords or codes. The scenario also shows that different security systems are used for different purposes.

Later, at work, Paul receives alarming information that something is wrong at home, but he does not know what. This obviously creates a feeling of loss of control. He soon finds out that he is being digitally blackmailed (a new crime, or rather an existing crime in new clothes). Then, there is the situation where Paul meets his boss following an informal police check caused by inadequate profiling. The search for all digital information on Paul highlights a disproportionate reaction to a suspicion based on only a profile match of 35 per cent.

Scene 2: Shopping while being at work

Scene two tells the story of Maruja's preparing for a business meeting while communicating with her daughter and with Shopping Assistant Software (SAS). It provides examples of AmI vulnerabilities within a commercial context. In the first instance, the SAS does not find a suitable gift. In the second instance, it misinterprets the notion of funny in relation to a farewell present for a girlhood friend and gives sex-related suggestions. These suggestions would normally only be visible on Maruja's PWC, but she accidentally projects them on the big screen during her business meeting. It results in a dark situation that is not only embarrassing for Maruja but also leads to her losing a client and, consequently, an end-of-year bonus. The complexity of the technology in relation to the value the user gets from using it is in question here.

More vulnerabilities pop up when Maruja accepts the special offer, suggested by her daughter, to buy a computer game on a website that they did not check out properly because of lack of time. The result is that Maruja suffers from the consequences of powerful spyware used by this site to get access to personal data for building consumer

profiles without people knowing about it. That was exactly the objective of the promotion. It is a new crime called data laundering.

Another issue is related to control as shown in the situation where children seek to circumvent parental and teacher control over playing computer games at school and the work situation where staff are "controlled" during business meetings to the extent that what is said is automatically recorded. The latter instance, however, can result in a decision taken on the basis of incomplete information, i.e., information that is not recorded.

Scene 3: At the park

Scene three starts with Maruja's going to a park for her lunch break to disconnect from her disastrous business meeting. Unfortunately, she gets spammed continuously with location-based advertising as a result of a misinterpretation of her personal profile. The avatar makes mistakes (Chinese food), is not informed (sandwich lunch) or gets influenced (low price restaurant). It shows that people can be irritated and annoyed by certain AmI applications. Maruja decides to switch off temporarily but later she regrets having missed a call from her boss and not being aware of the nearby presence of a friend.

Her friend Claire goes through a much worse situation because she is robbed while working in her apartment. The high-tech criminals did not expect her to be at home. By reading the RFID tags on Claire's blouse and by hacking[31] the client database of the shop that sold the blouse, they were able to determine the location of her apartment. The criminals did not know that Maruja, not Claire, was wearing the blouse. Claire not only suffers physically and financially from the crime but also needs to invest time in retraining her PWC again because she did not have her profile stored online. Although it was saved locally on her PC, the burglars wrecked her machine.

In the park, Maruja encounters a foreign visitor asking for the whereabouts of the central market. Maruja is surprised by the request because she (Maruja) would never go abroad without her location device. Maruja does not realise that this woman did not have a choice because of a lack of a roaming agreement between their respective service providers. Another issue is raised in the last situation in which Maruja reflects on theft of her electronic purse in a dangerous neighbourhood. While AmI technologies allow the update of neighbourhood crimes rates and guide users out of such places, they still depend on the business models supporting such applications. Maruja did not know because she forgot to authorise the update of her location software.[32]

2.2.2 AmI technologies and devices

The scenario makes reference to several AmI or AmI-related technologies:

- sensors and actuators
  - embedded in the environment and in objects, such as the sensors in Paul's

[31] Krebs, Brian, "Teen Pleads Guilty to Hacking Paris Hilton's Phone", *Washington Post*, 13 September 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/09/13/AR2005091301423.html

[32] See recent experiments with so-called Map Mash-Ups, combining geographical visualisation tools such as Google Maps with other data such as local crime statistics: Wade Roush, Killer Maps, www.technologyreview.com, October 2005.

study used to monitor physical presence and actuators that close the door after a while for security reasons,
    - RFID tags attached to clothing (readable from a distance) with backward traceability to the shop which sold it,
  - indoor and outdoor positioning devices
- biometrics including a fingerprint reader to open the door of the study and an iris scanner to authenticate online identity (which Ricardo manages to spoof because the model did not yet contain liveness testing),
- interfaces
    - smart clothing, e.g., the blouse that has an integrated flexible screen,
    - speech and voice recognition
- intelligent algorithms
    - for data mining (e.g., used by police)
    - speech recognition
    - Web search algorithms
- a Personal Wrist Communicator which is a multi-functional (phone, watch, camera, colour display) personal intelligent device,
- wireless, wireline and broadband communications networks.

2.2.3 AmI applications

The AmI technologies referenced in the scenario are used in various applications:

- security: restricted and authenticated access to Paul's study via a fingerprint reader and to his online profile via an iris scanner; automatic closing of a door when the absence of a person is detected,
- remote surveillance of the home and other premises,
- digital rights management (DRM), e.g., a licence fee associated with an IP number to prevent illegal copies,
- audio tracking of meetings and automated transcription into text;
- SAS: Shopping Assistant Software having intelligent search capabilities for e-commerce,
- powerful spyware programs to detect personal profiles,
- personalised advertising,
- seamless migration of content on different platforms/screens, from a PWC to big screens but only when explicitly authorised (and this went wrong in the case of Maruja as a result of hasty decision),
- new crimes such as digital blackmail, determining the presence or absence of people by reading RFID tags incorporated in clothing and other objects, crime information networks (e.g., Google Earth combined with local crime statistics),
- temporary online offers for quick decision-makers,
- location-based services
    - automated priority settings on incoming messages (e.g., Paul in his boss's office; Maruja during her business meeting)
    - advertising.

2.2.4 Drivers

Drivers for the AmI technologies and/or dark situations elaborated in the scenarios are the following:

- *Tele-work* (working from home): Although tele-work's importance and prevalence have been predicted for some decades, AmI might give a boost to it, not only because of the availability of high-bandwidth infrastructures but also of its user-friendliness, media richness and proximity to face-to-face interactions (although these are still needed, as mentioned in the scenario).
- *Convenience*: The AmI home addresses human weaknesses (via sensors and actuators) such as forgetting to close a door or window or to put out the lights or to turn off the cooker, etc.
- *Parental control*: The adoption of AmI technologies may be stimulated by those who seek greater parental control of children and, in particular, their access to services, drinks, entertainment, etc. On the other hand, clever children such as Ricardo may try to circumvent control mechanisms in order to engage in ID theft within the family.
- *Crime*: Criminals may see AmI as offering opportunities for new forms of old crimes such as blackmail (on a small scale involving many people for small amounts of money) by intervening into personal and home networks; data laundering (personal profiles for which people are willing to pay money); robbery (of, for example, electronic purses or by means of the remote detection of the presence/absence of wealthy individuals); exploiting weaknesses in AmI crime information networks such as a well-known weakness in the security of personal and home networks when rebooting.
- *Security*: Individuals, groups and societies will see benefits from AmI-based services such as remote surveillance as enhancing protection of physical premises as well as protecting their online identities.
- *Personalisation*: Based on personal and group profiles, AmI will be driven by, inter alia, companies who see opportunities for better market penetration through the provision of personalised services such as suggestions for shopping (e.g. Shopping Assistant Software); for eating (e.g. restaurants) and for matching personal profiles with location-based information. Personalisation is also likely to be an important driver for individuals as well, who will enjoy the benefits of services specifically tailored to their interests, needs and desires.

2.2.5 Issues

The scenario raises several issues by showing what can go wrong with AmI in everyday life. Many of them have to do with human factors such as failing to take adequate measures and feelings of loss of control.

Human factors and security

Human factors such as excitement can cause people to forget things (closing the door of the study), but AmI can help address the consequences (closing the door, locking access to online services). As security studies show repeatedly, however, human errors constitute major security weaknesses. AmI will certainly help to overcome this problem, but it would be naïve to assume that human failings could be factored out completely. Since not everything in the smart house will be accessed via biometric verification only, people will continue to use easy-to-guess or accessible passwords and/or access codes.

Remote surveillance of the smart home is not enough to secure it. Security requires on-the-spot checks and back-up systems if something goes wrong. False 'automatic' alarms

could be an issue in the future to the extent that they become counterproductive and ignored.

Other vulnerabilities are depicted as, for example, when Maruja accepts the special offer, suggested by her daughter, to buy a computer game on a website that they did not check out properly because of lack of time.

Dark feelings (loss of control)

Dark feelings can range from irksome to burdensome; and entail annoyance and embarrassment. Although AmI is supposed to be seamless and only visible when we want it to be, it can be assumed that it also occupies our minds since settings have sometimes to be confirmed or changed. AmI cannot know everything. It has to be fed information, which places a burden on people. Also, when AmI does not function as it should, people will get annoyed, possibly leading to their temporarily rejecting it (switching off). Annoyance can be foreseen when AmI does things that are not expected or wanted, even if authorised (willingly or unwillingly). All this contributes to a feeling of loss of control.

This is shown in scene 1 when Paul receives an alarm from his home system but without details on what is happening. It is an important downside when AmI is not behaving as expected while we depend on it. In addition, this alarm was a false alarm because of a digital blackmail generating stress and loss of trust, which are related to loss of control. More examples are raised in scene 2. First, Maruja got an unexpected message on the same screen as her business presentation. Second, the content of the message was sex related due to a misinterpretation of the notion of funny by the AmI service (Shopping Assistant Software), which results in annoyance and embarrassment. Finally, in scene 3, Maruja was irritated because her avatar was not able to take into account her preferences and she was worried because she did not know how to check the state of her avatar or how to inform it.

Control

Another issue is related to control as depicted in the situation where children are looking to circumvent parental and teacher control over playing computer games at school and in the work situation where staff are controlled by automatic recording of what is said in meetings. As stated above, this can result in a decision taken on the basis of incomplete information, i.e., information that is not recorded.

Disproportionate reaction to suspicions

In the situation where Paul meets his boss who informs him about police check, we see a disproportionate reaction caused by inadequate profiling. The police want to search all digital information on Paul based on a profile match of only 35 per cent. Since so much data are available on individuals, the police can do digital searches of publicly available data, before asking for a search warrant. Such public data can be used to match with criminal profiles. The risk is that it leads to innocent people such as Paul being treated as potential criminals, which in turn may have negative consequences, which in Paul's case means missing a promotion, even if afterwards the person is found to be innocent.

Insider ID theft

Ricardo is able to use his father's identity to bypass the parental control system and to shop and gamble online. This example shows that ID theft is possible without criminal intentions, that people who know each other can also breach privacy (the so-called "little brother" phenomenon) and that once identified, it is easy to spend money because payments are automated (up to a limit).

Exclusion

People may still be without certain AmI services (e.g., the foreign woman in the park in scene three). In this case, the woman was deprived of having personalised location-based services abroad because of a lack of an agreement between service providers. She can still receive location-based advertising that is "broadcast" even if her profile is not known. She would have been able to download city tourist information (including maps) as well but as a result of the lack of a roaming agreement between services providers, she could not have this information.

2.2.6 Legal synopsis

Privacy at home and in work place

An AmI world contains important challenges to the protection of privacy as we know it today. A first important issue is the distinction between the private life and the professional life. As this scenario shows, the borders between both will increasingly evaporate: people will increasingly work at home and in the professional environment people will deal via distant communication with private issues. All of this is closely connected to the fact that the different spaces which exist today will be interlinked and articulated. In AmI, we might face the need to redefine or reinterpret the terms home, communication and private life. Although the European Court of Human Rights accepts the protection of privacy in the working place, and has introduced the notion of "reasonable expectation of privacy" which applies also to the working sphere, it is still unsure how it will apply in AmI. Another important challenge to privacy is the fact that new tools of monitoring and profiling will appear in an AmI world. An example of such a tool is Digital Rights Management (DRM). Although this tool is initially meant to ensure the protection of copyrights, it can be used to monitor consumers' behaviour and preferences. Another important tool is spyware. The application and use of such software might violate important principles of data protection law. It may also constitute criminal offence.

Data protection and liability

In a world where everything will be interlinked and information will move between different spaces, it is important to ensure the protection of this information. We also need secure systems in order to be able to conclude contracts over networks. Several legal instruments put important security obligations on service providers. The compliance with these security obligations is, however, not clearly regulated and there is an important problem of enforcement. When damage is caused because of inadequate security, the crucial question is: who can be held responsible? When two or more service providers are involved, the victim will have difficulties in determining who is

specifically responsible for a security breach. Similar problems may occur in the breach of the security of the home network used for work purposes. This should not, however, prevent the injured party from recovering damages. Protection of consumers against unwanted aspects of e-commerce and distance contracts, as well as against unwanted commercial messages should be enhanced.

Inadequate profiling and data laundering

In an AmI world, service providers will try to collect the maximum amount of information, in order to be able to provide personalised services and communications. Such processing of personal data, however, also entails important risks. Data processors should be careful not to process incorrect information, since this might cause important damage to the data subject. Also, profiling will play an important role in facilitating AmI services. That makes the dangers of incorrect or incomplete information even bigger. Although data protection law provides mechanisms to protect the data subject, it is crucial to ensure that these mechanisms are enforced. Data subjects particularly need to be protected against decisions based solely on automated processing of their data.

EU Directives 95/46 and 2002/58, which foresee these mechanisms, do not apply to the use of profiling techniques by the police or in other 'third pillar' related activities. This lacuna may need to be addressed.

The enforcement of data protection could be challenged by the practice of 'data laundering', where (similarly to “money laundering”) a large uncontrolled and untraceable (commercial) traffic of individual profiles and personal data could become one of the “escape routes”. Some specific measures might be envisioned here, such as specific incrimination and the creation of a duty to notify substantial acquisitions of personal data.

Criminal liability

The Cybercrime Convention penalises the illegal access and illegal interception of computer systems or data (like accessing the information contained in the RFID-blouse). This harmonisation, however, is limited in substance (countries may impose extra conditions for an act to constitute a criminal offence) and territory (a limited number of countries have ratified the Convention).

2.3 CONCLUSIONS

This scenario depicts AmI vulnerabilities in the life of a typical family, in different environments – at home, work and a park (a public space). It implicitly indicates mobility of users and hence of AmI services in and through different spaces. The scenario gives an idea of some of the potential benefits of AmI services but the core focus is on threats and vulnerabilities that may lead to critical situations or so-called dark situations related to inconvenience, control, crime, security and profiling, among others. This scenario also raises important issues such as human factors and security, dark feelings, especially loss of control, disproportionate reactions based on ill-founded suspicions, identity theft and exclusion.

3 DARK SCENARIO 2: SENIORS ON A JOURNEY

3.1 THE SCENARIO SCRIPT

Introduction

As a former software engineer, Martin Schmitt, born 1943 (aged 77 in 2020), is familiar with technology. His wife Barbara is 75. The Schmitts have lived for more than 10 years in a village in the alpine upland that has been specifically designed for senior citizens and is equipped with ambient intelligence technology. For their age, they are both healthy. The Schmitts' daughter Heike has her own family now and they live in northern Germany. Heike sees her parents only once or twice a year, but maintains contact during the rest of the year by means of AmI. The Schmitts are participating in a typical travel program for senior citizens to Florence, Italy.

Scene 1: News from the police report: Senior citizen dies after bus accident

Florence – Twenty-four senior citizens were injured in a bus accident on a sightseeing trip Friday afternoon. An 84 year-old woman died under tragic circumstances.

According to Florence police reports, the bus was on a sightseeing trip with 46 senior tourists from Germany and Austria when for unknown reasons the traffic lights at a major intersection went to green for all directions. The bus driver avoided a collision with the oncoming traffic but knocked down some traffic signs, went off the street and finally crashed into a lamppost.

Fifteen of the passengers on the bus had minor injuries and were released from the hospital shortly after. Nine were more seriously injured and had to be treated stationary at the Careggi Hospital. Though the emergency service arrived quickly, the severe internal injuries of an 84-year-old woman from Austria remained undetected because she used an outdated health monitoring system. She died on the way to the hospital.

Automated alarm messages from HMDs

Heike Lengbacher-Schmitt is sitting in the subway on her way home when she suddenly receives two alarm messages on her personal wrist communicator (PWC). Her parents' health monitoring devices (HMD) issued the alarms, indicating that a critical situation had occurred.

Of course, Heike becomes concerned. She had picked up similar messages before from one of her parent's HMD, and in all of these instances things eventually turned out to be fine. But this was the first time she received alarms from both parents at once. Moreover, she knows that her parents are on a bus tour, making the situation even more worrisome.

No direct contact

Heike's attempts to call her parents are not successful. As she learned later that day, in an emergency situation, the HMDs by default block any incoming communications from people not directly involved in the rescue efforts in order not to disrupt the immediate rescue process. And during the examinations at the hospital, mobile communication

devices are required to be turned off.

Over the course of the next three hours, she leaves numerous messages at her parents' digital communication manager, urging her parents to return her calls as soon as possible.

Superfluous, decontextualised information

In addition, Heike accesses her father's personal data storage. The system recognises her and, because she was granted comprehensive access rights beforehand, releases large amounts of information such as geographic locations, stopovers, local temperatures, etc. All of the impersonal and unspecified information raises even more questions, however, making it very difficult to grasp her parents' situation. Heike is not really relieved by the data, on the contrary. At least, she eventually finds out that her parents are at the Careggi Hospital in Florence. After phoning the Hospital, Heike is informed that her parents are receiving medical treatment.

After Martin Schmitt has been thoroughly examined, he is allowed to leave the emergency room and turn on his communication devices again.[33] He immediately calls his daughter.

Phone call

Heike: Hello? Oh, it's you, dad. Thank goodness! Are you all right? How's mom? What happened?

Martin: Don't worry honey, we're fine. Our bus had an accident, and your mom was slightly injured, nothing serious. She has a slight concussion and I have a few scratches. Nothing to worry about, believe me.

Heike: Can I talk to her?

Martin: Sorry honey, but she's still being treated and the doctors said she should not be disturbed.

Well meant services act against the user's will and may have rebound effects…

Heike: By the way, Aunt Anna called me just a few minutes ago. She was totally freaking out because she received the same alarm messages as I did. Apparently she became so excited that her HMD even alarmed her doctor!

Martin: Oh no, I forgot to take Anna off the list of people to be automatically notified in an emergency. Please call her for me and try to calm her down. Listen, I want to go back to your mother. I'll call you later. Just wanted to let you know everything's okay.

Heike: Tell mom we're with her. And don't forget to call me; I have to know what happened!

---

[33] At the moment it is debated if wireless technology can be banned from hospital any longer or if "wireless tagging is 'inevitable'". Carr, S., "Wireless tagging in hospitals is 'inevitable': Prepare to be chipped...", silicon.com, 7 December 2004.
http://hardware.silicon.com/storage/0,39024649,39126387,00.htm

Video messages

As it is already past midnight when Martin finally leaves the hospital, he decides to send a video message to his daughter instead of calling her. In his hotel room, Martin sets up his mobile phone in front of him and starts recording his message. He also attaches a short clip showing Barbara in the hospital, saying a few words to reassure her daughter. Martin had ignored the ban on using mobile recording devices in the hospitals and filmed a short video-sequence of his wife anyway.

Dear Heike! As you can see, I'm absolutely fine. And your mother is recovering quickly. She will be released tomorrow morning. But let me tell you what happened from the beginning.

Scene 2: Travel preparation and check-in procedure for public transportation

Travel preparation

Unlike our normal habit, Mom and I actually had completed travel preparations way ahead of time. So there was no need to get stressed out. And thanks to the travel-assistance procedure of the AmI environment in our home in Murnau, this time we even thought of recharging our PWCs and HMDs early enough to avoid losing "our identity" like on our last trip.

Disclosure of location information violates privacy and results in embarrassing situation

In Munich, I experienced an awkward situation after I located a former colleague of mine using the "friend-locator" function (LBS) of my PWC.[34] *I just wanted to say "hi", but when I walked up to him, I was surprised to see that he had a good-looking, younger woman with him who obviously was not his wife. He blushed, mumbled a few words and disappeared in the crowd. It seems difficult to keep secrets these days...*

Boarding the bus

At Munich station, we met our old friends Brigitte and Peter as planned. The four of us proceeded to meet up with the travel group in the new bus terminal, just next to the station.

After Alessandra, our Italian tour manager for the next days, had welcomed us to the tour and introduced herself, we finally started to pass through the security gates in order to board the bus.

Feeling uneasy - loss of control

Denial of transportation

I guess I'll never feel comfortable with all these safety measures you have to endure when travelling: biometric ID verification,[35] *detectors for drugs and explosives, etc., especially if they reject you erroneously.*[36] *Imagine, one of our fellow travellers, Michael from Baden-Baden, was denied access to the boarding area of the terminal, although he had a valid ticket and even could present the receipt from his travel agent!*[37] *Apparently, some kind of data mismatch between his*

[34] Paciga, M. & Lutfiya, H., 2005.
[35] Bolle, R., et al., 2004.
[36] Maghiros, I.; Punie, Y.; Delaitre, S. et al., 2005.
[37] Schneier, B., 2004.

Resistance	*personal ID, the e-ticket and the information stored on the central server had caused the problem.*
Legal discrimination	*The security personnel at the terminal were absolutely stubborn and unwilling to make an exception, despite several interventions by Alessandra and Peter, who, by the way, is a good friend of Michael. The officials urged Alessandra to accept the situation and told her to leave without Michael. But they hadn't reckoned on the solidarity of the whole group – we made it unequivocally clear that we wouldn't leave behind a member of the group. Actually, I was surprised myself that nobody of our party stepped out of line.* *Imagine. Michael was obliged according to the law to receive a "possible risk status for an unlimited time" because he is causing more security risks than normal. He has to accept this "possible risk status", granted to him by the officer, which means that all his actions and movements are followed and stored, including his presence, actions and movements.*
Liability	*To make a long story short, it took about another hour until Alessandra had worked out an agreement with one of the senior officials. The solution was that the tour manager and all passengers had to sign a statement discharging the bus terminal of any responsibility for possible damages caused by Michael. Pretty ridiculous if you ask me, especially considering that once you leave the terminal, anybody can hop on the bus without any security checks at all!*

Scene3: Traffic supported by ambient intelligence

Mobile entertainment systems	*After a pleasant stopover in Bolzano, we continued our journey the next day. The ride through Upper Italy was uneventful. Some of us were watching on-demand videos or reading books on their portable screens.*[38] *And Alessandra turned on the interactive tour guide of the bus that explains what we could see outside the bus if it had not been so foggy in the Po lowland. Instead, some videos of the scenery were projected onto the windowpanes.*
Traffic jam situation	*Later on, our bus driver even managed to by-pass a major traffic jam on the highway near Modena. Well, actually he just had to follow the instructions he received on his on-board navigation system. Within seconds after the potential disruption of the traffic flow – later we learned that a severe accident had occurred about 30 km ahead of our position was detected by the traffic monitoring system – a traffic warning and, almost simultaneously, an alternative route were issued.*
Cognitive overload	*Thanks to the intelligent filtering system, our driver was able to take the decision at the right moment without being distracted by too much*

[38] Espiner, T., "Philips unfurls prototype flexible display". http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39216111,00.htm

avoided	*information while driving.*
Business model:	*Luckily, the bus company we were travelling with had subscribed to one of these expensive premium traffic information schemes. Many other people travelling in the same direction weren't as fortunate as we were.*
Traffic control system	*In Florence, traffic volume was pretty high, but considering the rush hour, we moved along quite smoothly. The electronic road signs told us that inbound traffic was given priority. In addition, our bus had permission to use the lane reserved for public transport. Paying tolls is always undesirable, but these urban traffic management systems seem to pay off.*

Scene 4: Emergency situation

Malicious attack against traffic system[39]	*But then again, the traffic management systems are far from perfect. The accident we were involved in was, as we learned later on, caused by a kid who illegally used software for priority vehicles like ambulances and police cars.*[40]
	All of a sudden, cars coming from the right entered the junction at high speed. In order to avoid a collision, our bus driver pulled to the left and we ran into the central reserve, hitting all kinds of signs and objects. Finally, we crashed into a large lamppost and came to a brutal and sudden stop.
(medical) reassurance thanks to AmI	*It took me a few moments to realise what had happened and to regain orientation. Your Mom was obviously unconscious because she didn't respond to me. So I checked her HMD immediately. The display indicated that an emergency call had already been issued. Thank goodness, all vital parameters such as blood pressure and pulse rate were okay.*
Selling surveillance pictures/videos to the media	*I looked around and saw the mess we were in. You should see the camera images taken in the bus (as you know, the cameras in the bus record everything constantly), but they were not immediately available because the bus company gave commercial exclusivity to a television station… So we have to wait until the police give us a copy, if we ever get one.*
International interoperability,	*What I did not know was that some passengers were using HMDs that are not compatible with the Italian system. Thus, they were not able to*

[39] Poulsen, Kevin, "Traffic Hackers Hit Red Light", *Wired News*, 12 August 2005. http://www.wired.com/news/technology/0,1282,68507,00.html

[40] In summer 2005, the US government outlawed the possession of "traffic signal-pre-emption transmitters" after hackers had used them to manipulate traffic lights. Poulsen, K., "Traffic Hackers Hit Red Light", *WiredNews*, 12 August 2005. http://www.wired.com/news/technology/0,1282,68507,00.html.

download the health information of a couple of people on the bus and the semi-automatic rescue co-ordination centre assumed there were only 32 people on board and sent too few ambulances. This did not have severe repercussions since many of us were not seriously hurt.

System cannot distinguish reason and effect

The police, ambulances and fire brigade arrived rather quickly. The fire brigade, however, was not needed. It was called because the alarm signal stopped after three minutes due to a power shortage in the vehicle and the rescue centre interpreted this as an indication that the bus might have caught fire – the travel organisation will have to pay for this service, but who wants to grouse?

AmI divide!

On their way, the paramedics had checked the medical records of the passengers and the HMD signals and set up a list of people with more serious injuries and those with private health insurance.[41] Apparently, they were given priority treatment and transport to the hospital. Too bad we didn't opt for such insurance and had to wait for more than half an hour before being examined.[42]

Exchange of identity

A "funny" incident happened when my neighbour was almost given an injection just because he had not picked up his own but someone else's HMD.

Service quality and system update or even opt out

Delegation human decision to technology

But something really tragic occurred with Monika Klein, a nice 84-year-old lady from Salzburg. She was one of those whose health insurance refused to pay for an update of the HMD to the latest model; and the paramedics had neither her patient record nor her current vital data. When one of the paramedics walked around and talked to those who were not on his automatically-produced list, she told him that she was not in pain, only exhausted. Because there weren't enough ambulances at the scene, they left her sitting on a bench next to the road. Since the introduction of HMDs, these guys depend too much on the technology. They are not even able to practice the simplest diagnosis. Otherwise they would have diagnosed that Mrs Klein had internal bleeding. I heard that when they finally decided to take her to the hospital, one of the last to go, she suddenly lost consciousness and passed away before the ambulance reached the hospital.

Scene 5: Ambient intelligence and medical care

Pressure to disclose personal data

After we arrived at the hospital, I had a fierce argument with the lady at the reception who complained that she was not able to access my health and insurance record completely. The doctors, she said, were unable to help me if I wouldn't disclose my complete data to the hospital.

Data leakage –

Heike, you probably remember that I had forbidden the health services

[41] Michahelles, F., Matter, P., Schmidt, A., Schiele, B., 2003.
[42] Carr, Sylvia, "Wireless tagging in hospitals is 'inevitable'. Prepare to be chipped...", Silicon.com, 7 December 2004. http://hardware.silicon.com/storage/0,39024649,39126387,00.htm

illegal trade with personal data may lead to spamming

to give away certain data because I had been flooded with drug advertisements last year after that scandal with the illegal trading of personal health data. I saw no necessity to give the hospital complete access since I only had some scratches. However, I had to sign a statement that the hospital is not liable for any impairment resulting from their treatment.

I really wonder if the benefits of automated health care are really worth this mess. I promise to keep you posted. Say hi to George and hug the kids for us!

Bye for now!

3.2 ANALYSIS

3.2.1 Situations

The scenario presents three different environments that reveal possible weaknesses related to public or semi-public infrastructures and the trade-off between economically efficient procedures as implemented in AmI services and the variety of individual needs.

Citizens must be able to trust and rely on unfailing operation of these infrastructures – especially for vital functions. Fair access and user-friendliness are needed to prevent an ambient intelligence divide. While equal and fair access is the basic requirement for the possibility to use public utilities, user-friendliness is the core factor for the actual use of AmI services. In this respect, disabled and elderly people have a particular demand.

Scene 1: Framework situation: AmI-supported communication

This scene depicts communication links between an elderly person and his children living far away.[43] Synchronous and asynchronous communication using text, phone or video from basically any location is assumed to be standard. For both the elderly father and his daughter, these communication possibilities are part of everyday life, including receiving all kinds of information automatically issued by personal agents such as HMDs. In an emergency situation, however, automatic alerts can actually cause more harm than good unless they inform the recipient adequately about the situation.

Scene 2: Travel preparation and check-in procedure for public transportation

This scene shows the preparation of the elderly couple for a short trip. The scenario assumes that elderly people remain active up to an advanced age and are supported by AmI technology in their daily activities, including travel preparations.[44] AmI-enabled services can remind users not to forget important things (like an HMD).

In the aftermath of 9/11 and other terrorist attacks in recent years, boarding public transportation usually involves more or less extensive procedures of identification, control and surveillance. People have to get used to it. The imperfection of technology periodically leads to nuisance and sometimes even to open insubordination when results are *obviously* faulty and authorities deny services. An open issue in this respect is the trade-off between public security and individualism.[45]

Scene 3: Traffic supported by ambient intelligence

This scene explores the delicate balance between market- and supply-driven approaches to many new mobile services enabled by the availability of personal information in fields that are considered public utilities today. This development may result in a decreasing relevance of free and publicly available services and in a growing disparity

[43] As presented in Cabrera, M. and Rodríguez, C., 2005.
[44] See, for instance, Cabrera Giráldez and Rodríguez Casal, 2005, and Korhonen, I., Paavilainen, P. and Särelä, A., 2003.
[45] See, for instance, Fujawa, J. M., 2005.

between those who can afford the benefit offered by ambient intelligence and those who cannot.

Extrapolating from current developments, we can assume that bus drivers (like other traffic participants) will be supported by numerous AmI applications to make driving more efficient and less stressful. Avoidance of traffic jams will be one of the most popular applications (which won't be surprising considering the experiences made in the late 20th century). As some of these services constitute business models, quality and speed of traffic information services differ according to the price consumers are willing to pay.

AmI technology also supports passenger activities Such as individualised entertainment (video, music, interactive games) and edutainment like an electronic tour guide, which gives explanations about the scenery outside (augmented by videos and other multimedia).

AmI technologies will be an important element in large cities' efforts to come to grips with unbearably high traffic volumes and recurrent congestion. Traffic management systems constantly monitor and manage traffic flows according to predetermined parameters through centrally controlled traffic signs, traffic lights and other electronic means of traffic management. Certain vehicles such as ambulances, streetcars, buses, taxis, etc., are granted priority rights. Traffic management systems can be deceived, however, by illegal hardware and software.

Scene 4: Emergency situation

Public authorities have established AmI-supported emergency systems with automated information chains from the individual person and vehicle to the emergency services (police, ambulances, hospital).[46] This has become a complex system, since heterogeneous actors and systems have to communicate seamlessly. Given the fast development of technology, different national standards and health systems, this system remains imperfect – services cannot be offered to all citizens in the same way. In addition to the problems associated with operating efficiency, health and emergency services become increasingly differentiated from basic to premium services, creating an "AmI-divide". For whatever reasons (e.g., because they are using older equipment, live in regions without technical coverage, or even have opted out), people who remain outside the system are at risk of not even being provided with the most basic services.

As for other applications, AmI-enabled emergency systems may be driven by market forces making differences between people who can afford a premium service and those who cannot. While this is already taking place in the existing health insurance system, it is a sensitive issue who is actually driving the development: the insurance companies and health care suppliers who are under constant pressure to act economically and efficiently or citizens (represented by the government) who set the rules and define boundaries for AmI health care services.

In addition, identities can easily be mixed up if the link between a person and his/her personal device is dissociated (e.g., picking up the wrong HMD).

[46] Savidis, A., Lalis, S., Karypidis, A. et al., 2001.

Scene 5: Ambient intelligence and medical care

This scene reveals vulnerabilities like those in the emergency situation. Hospitals ask for a complete disclosure of health information (regardless of the need for the actual treatment) in order to be on the safe side and avoid liability. Again this poses the question about who is in control of the system and who establishes the rules that apply to denial of services.

In order to reduce possible interference with medical procedures and to protect the patients' privacy, all mobile communication devices are required to be turned off within hospitals.

3.2.2 AmI technologies and devices

This scenario makes reference to several AmI technologies:

- Sensors and actuators
  - embedded in the environment and in objects and attached to people, such as an impact sensor for accident detection and body sensors measuring the vital parameters of the elderly (or people with health risks)
  - detectors of drugs and explosives
  - positioning
  - biometrics
- Interfaces
  - portable screens
  - augmented reality displays (such as bus windows)
- Intelligent algorithms for
  - priority-based traffic routing
  - routing of network traffic in emergency situations
  - processing of health data in real time
  - detection of persons with highest health risks or best insurance
- Communications networks enabling seamless service by heterogeneous devices with/without central control providing greater coverage (especially for emergency communication).
- (Personal) Health Monitoring Devices (HMDs), which are health-related personal intelligent devices and which could be combined with other multi-functional devices such as a Personal Wrist Communicator.

3.2.3 AmI applications

Scenario 2 refers to various AmI-enabled applications including the following:

- *Personal communication management system*, like that described in ISTAG's "Dimitrios Scenario"[47], control the communication of the elderly couple based on the context, e.g., it denies communication in the emergency when communication with the authorities has priority and at the hospital where mobile communication devices are not allowed. On the other hand, it proactively sends messages to family members and recognises people close by ("friend locator").
- *Support system for elderly people* helps to enable an independent life to an advanced

[47] ISTAG, Scenarios, 2001.

age. This system reminds users about tasks to be done and objects to taken with them. When coupled to a health monitoring system, it also supports a healthy lifestyle.

- *Check-in and security procedures* for public transportation are technically integrated to a large extent, combining access controls with identification procedures (supported by biometrics and central databases) and security protocols. If operating accurately, the system speeds up regular check-in procedures and helps to detect potential security risks.
- *Personal health monitoring systems* survey vital parameters of people with certain risks such as high blood pressure or diabetes. The collected data can be used either by a physician for routine examination or in an emergency. The personal health monitoring system may be linked to a health insurance database and a communication system.
- *Public traffic management systems* collect information about the current traffic and give support to road users either collectively or individually. The business models may vary from free public information to pay-per-advice models.
- *Automated emergency alarm systems* can detect accidents and the urgency of the situation (especially if coupled with the personal health monitoring devices of the drivers and passengers). The rapid alarms and automated requests for assistance improve the quality of the medical system and help to reduce traffic casualties.
- In a *seamless medical information system*, all relevant information is collected, including personal medical history items such as prior illnesses, treatments and medication as well as up-to-date vital information and information about the health insurance.

3.2.4 Drivers

Each of the AmI technologies mentioned in the scenario has been driven by a set of two or more interdependent factors. Analytically, the following drivers can be distinguished:

- *Political*: The introduction of some of the most important AmI applications in the scenario has largely been driven by political objectives such as reducing the risk of terrorism (security), improving the efficiency of the health care system (emergency), and the improvement of the traffic situation in urban areas (public infrastructure).
- *Commercial*: Numerous AmI services such as the “friend-locator”, multimedia applications on the tour bus, individually tailored traffic information and automated communication links are primarily driven by profit motives and the (successful) development of business models.
- *Diffusion*: Especially in mass consumer markets, high penetration levels of basic communication technologies constitute an important vantage point for the demand for complementary services such as video-based communication or automated and personalised information exchange.
- *Accountability*: Both the boarding procedures at the bus terminal, which proved to be quite humiliating for one of the group members, as well as the fact that hospital patients are required to disclose their complete personal health data, are based on the institutions’ objective to reduce liability as far as possible.
- *Illegitimate personal advantages*: As AmI technologies regulate access to scarce goods, people may be motivated to seek personal advantages by circumventing standard procedures and/or by using technical solutions to deceive the system (in the scenario: priority rights in traffic management system). Perpetrators might take into account possible hazardous consequences (because they seek to cause those

consequences) or they might not (because they are ignorant of the consequences).

3.2.5 Issues

In view of the above-mentioned vulnerabilities of ambient intelligence in travel/mobility and health care applications, we can identify certain issues that are critical for AmI applications that rely on large-scale public infrastructure and have largely the character of a public utility:

Dependence

Automated alerts are not necessarily beneficial – they may even cause more confusion because alerts reach the addressee immediately, but direct communication with the victim is often no longer possible.[48] The promise of permanent accessibility leaves the user helpless when communication is needed but not possible.

Privacy

What is the necessary degree of disclosure of information? In a normal situation even the disclosure of simple data (e.g., location) may violate privacy, whereas in other cases, the revelation of more information of the same kind may be warranted. Thus, the degree of information disclosure depends on the person, context and situation, which poses a challenge for the design of adequate communication rules.

Loss of control

If certain activities rely on the proper operation of technical systems, a feeling of uneasiness and loss of control may occur if it is not transparent to the citizen why a certain decision is made, especially when common sense suggests a different decision.

Risk and complexity

If AmI systems that are vital for the public (such as in emergencies) are known to be vulnerable or that don't cover the whole population, a "conventional" backup system, which provides at least a basic level of service, is needed.

Safeguards

Responsibility is moved to the weakest link in the chain, normally the citizen. In cases in which users do not adapt fully to the system requirements (e.g., provision of data); a liability may be generally refused – even if it has nothing to do with a certain damage or harm.

Exclusion

Services that are regarded as public utilities today may become commercialised. Even if the common welfare is increased, there is the risk of more inequality and even a loss of benefits for certain social groups (AmI divide).

[48] Savidis et al. 2001 assume in their scenarios that the personal communication device is deactivated for public communication in order not to disrupt emergency relief activities.

Identity

The loss and/or confusion of identity may not only be the result of malicious identity theft, it can also occur by mistake if the identification of a person is merely based on a detachable personal device.

Crime and complexity

Complex and distributed technical systems may offer new opportunities for illegal activities. This not only applies to property offences and terrors but also to misdemeanours and regulatory offences as well. Especially in those cases in which sensitive elements of the public infrastructure (e.g. traffic management) increasingly rely on AmI technology, even minor violations of the rules can unintentionally cause severe damage.

3.2.6 Legal synopsis

Conflict of laws

In an AmI world, people will be able to enjoy every service everywhere. In the scenario, an example is provided of how a group of elderly people is able to enjoy health and mobility services across borders. If an accident happens, however, it appears that important legal issues arise. Not only are many different service providers involved, these different service providers can provide their services from anywhere in the world. In order to be able to determine who will be responsible for the damage, we have to know which law is applicable and which courts will be competent. On the European level, solutions are provided both as regards contractual and extra-contractual (tort) liability, but they are not adapted to an AmI world.

When considering the criminal issues, the jurisdiction is still determined by national law. Although some instruments try to make uniform computer-related criminal offences, they remain limited in scope and only applicable to a few countries. The legal instruments related to criminal law also deal with people who indirectly make the offences possible.

Interoperability

In order to ensure the interoperability between the different services and systems, international standards need to be created. Both at the European and international levels, important efforts are required. The European Union provides for mechanisms to stimulate the Member States to co-operate with each other and with the Union. As shown by the scenario, this cannot solve everything. In order to be able to comply with international standards, everybody needs to have and to be able to afford the necessary up-to-date technology. In the instance of sensitive AmI services such as health and general alarm systems, it is unacceptable that some people could not enjoy them because of the fact that they can not afford the appropriate technology. Not being able to use the necessary health services might have fatal consequences. Stringent regulation should be imposed on health service providers and health insurance companies to guarantee everyone's access to the necessary technology.

Data protection

In an AmI world, huge amounts of information will be collected in order to provide personalised services. Several principles of data protection are very important. The first is the proportionality principle, which states that "the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed." However, this principle is obviously at risk in a high-speed society with constant data processing and systems becoming capable of intelligently processing and using large amounts of personal data. In other words, disproportionate data processing often takes place. Data processors must also ensure that the personal data is accurate, up-to-date and correctly processed. Effective methods to object to the errors in the data processing should be guaranteed.

Data processing can be made legitimate when the data subject gives her informed consent. The hospital example, however, shows that this consent is often not freely given because the data subject is in a subordinate situation. In more general terms, data subjects are subject to the power of the data controller, who possesses a good or a service to which they want access. When people refuse to consent to the collection of their data, this should not have a negative impact on their situation. The data subject can have legitimate reasons to refuse it (such as fear of spamming) and the hospital cannot limit its own liability because of this legitimate refusal.

3.3 CONCLUSIONS

The scenario about ambient intelligence in travel and health applications makes clear that even in fields with a quasi-public character; it is not self-evident that all citizens will benefit from the deployment of ambient intelligence as envisioned by policy-makers and scientists.[49] In fact, the complexity of large-scale technological systems for traffic management and public health show that careful steps have to be taken in order to balance public and private interests – ranging from government, commercial network and service providers to the individual citizen and civil society as a whole.

It is a great challenge to avoid unjustified and excessive drawbacks or benefits for any of the affected parties. The challenge requires a blend of legal, organisational and technical measures. On the technological level, interoperating systems with a high degree of dependability (supplemented in part by independent fallback systems) are needed when the individual or society as a whole depends on an operating system. On the organisational level, measures are needed to make (public) services transparent and trustworthy. Finally, the legal framework and the regulation of important public services have to be adjusted to new circumstances. This also means that existing networks and constellations of societal actors need to respond accordingly.

[49] See, for example, IST Advisory Group, *Ambient Intelligence: From Vision to Reality*, Luxembourg: Office for Official Publications of the European Communities, 2003. http://www.cordis.lu/ist/istag-reports.html. See also Emiliani, P. L. and Stephanidis, C., "Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities", *IBM Systems Journal* 44, No. 3, 2005, pp. 605-619.

4 DARK SCENARIO 3: CORPORATE BOARDROOM & COURT CASE

4.1 THE SCENARIO SCRIPT

Introduction

The Data Mining Corporation (DMC) has an almost perfect business model. It collects data about individuals from hundreds of sources[50] and then sells the aggregated data back to many of those sources. Its principal sources (and clients) include insurance companies, retail chains, media conglomerates, credit-reporting agencies, mobile phone companies, law enforcement agencies, customs and immigration authorities, and intelligence agencies.

The advent of ambient intelligence technologies – including RFIDs, networks of sensors and actuators, fourth generation (4G) mobile, surveillance and biometric technologies, and software that learns from our past behaviour and preferences to predict what we will want or will do[51] – has enabled DMC to construct detailed files on virtually every person in the United States, western Europe and other developed countries.[52] DMC knows what products we buy, services we use, who we are in contact with, where we are at any point in time, and so on. DMC can confirm whether we are who we say we are and what sort of activity we've been engaged in. Linking together many different databases and processing the acquired data using its own proprietary algorithm has enabled DMC to create such fine-grained profiling that it is the envy of its few remaining competitors.

Although DMC is a relatively new company, it has grown quickly. Among the ways it has managed to sidestep legislative and regulatory constraints on transfers of personal data is through mergers with or acquisitions of companies with their own extensive databases. It is headquartered in Miami, but now has major subsidiaries in London and Tokyo. It is listed on the New York and London Stock Exchanges and is considering a listing on the Tokyo Stock Exchange.

Scene 1: Management board meeting

Biometrics for identification & authentication	*The company secretary places his hand on a fingerprint reader outside the boardroom and then stands close to the iris scanner. The boardroom door opens and he enters. As he does*

[50] cf. O'Harrow, Robert, *No Place to Hide*, p. 124: "LexisNexis, a subsidiary of the UK-based Reed Elsevier Group, maintains billions of records, including media reports, legal documents, and public records collected from thousands of sources around the world."

[51] cf. Biever, Celeste, "RFID chips watch Grandma brush teeth", NewScientist.com news service, 17 March 2004: "Tiny computer chips that emit unique radio-frequency IDs could be slapped on to toothbrushes, chairs and even toilet seats to monitor elderly people in their own homes. Algorithms on the PC use 'probabilistic' reasoning to infer what the person is doing. For some tasks, merely picking up an object such as a toothbrush is enough."

[52] See, for example, O'Harrow, p. 222: "HNC…monitors 90 per cent of all credit cards in the United States and half of those in the rest of the world…using artificial intelligence to seek out indications of fraud and deceit." See also Solove, Daniel J, *The Digital Person*, p. 20: "Wiland Services has constructed a database containing over 1,000 elements, from demographic information to behavioural data, on over 215 million people."

Linking of technologies, personalisation *Resolving differences in preferences*	*so, the lighting and the air conditioning automatically come on and are set at his comfort levels which are known from his previous activity in the room. A second later, the door slides open and the DMC president walks in. The sensors and actuators in the boardroom slightly adjust the air conditioning and lighting to the midpoint between the president and secretary's preferences. The president nods a slight greeting to the company secretary who can see his boss is preoccupied. A few seconds later, the vice presidents enter one by one and take their seats, and the lighting and air conditioning sensors and actuators make further adjustments to the collective mid-point levels.*[53]
Holographic representation of AmI *Multifunctional displays* *Surveillance* *Failure of AmI tech to recognise someone*	*The vice president for media relations has not arrived. The president is petulant. "Where's MacDonald?" she barks at Alvin, the holographic embodiment of DMC's embedded intelligence. The boardroom video screen switches from the agenda and shows MacDonald's office. He is heard and seen finishing off a conversation with a journalist. He gets up from his desk and leaves his office. As he does so, another camera in the hallway shows him going down a corridor. His position co-ordinates, accurate to less than a metre, shown in the lower left-hand corner of the boardroom screen, change as MacDonald approaches the boardroom. He is seen putting his hand to the fingerprint reader, but the reader does not respond. He tries unsuccessfully to rub some ink from his finger, and then leans close to the iris scanner, which does respond, but he is still not admitted to the boardroom since he must have positive responses from both systems.*[54] *The impatient president commands Alvin to open the door and finally McDonald is admitted.*
Voice activation *Intelligent display*	*"Okay, let's get on with it," says the president. "Show me today's agenda," she instructs the computer. The agenda appears on a large wafer-thin video screen on the wall opposite the president. Three items are listed:* *Data from developing countries. (Switzer)* *Theft of data, 29 June 2015. (Perrier)* *Considerations re listing on the TSE. (Hausmann)*
Reliability of data *AmI not completely*	*Kevin Switzer, vice president for operations, speaks. "We've had complaints from the Customs and Immigration folks about the shortage and reliability of our data on people coming into the States.*[55] *It mainly concerns people from developing*

[53] On modelling group behaviour, see Masthoff, J., 2002.
[54] Jain, A. & Ross, A., 2004; UK passport service biometrics enrolment trial, May 2005. http://www.identitycards.gov.uk/library/UKPS_Biometrics_Enrolment_summary.pdf .
[55] cf O'Harrow, p. 48: "For years, the credit bureaus had been dogged by complaints. Information in their reports was chronically incorrect. They routinely failed to correct mistakes, and seemed arrogant when individuals called."

pervasive

AmI contributes to detailed profiling

Absence of AmI creates new digital divide

countries. With our profiling technologies, we are able to identify anyone who might be a security risk or disposed to anti-social behaviour. Unfortunately, most developing countries have no AmI networks, which makes it impossible to build up the same kind of detailed profiles of individuals like we can here in the US, Europe or Japan. So the immigration authorities have been making threatening noises about refusing entry to people from countries without AmI networks."
"So what are you doing about it?" asks the president.

AmI as an inducement, but…
who controls the data?

"Well, I think we have a golden opportunity here. We can offer to set up AmI networks in those countries as long as we, I mean DMC, are the ones to collect and process the data. You'd think most countries would jump at the chance to have networks put in place at virtually no or little cost to them, but some of the countries are quibbling with us."[56]

"Quibbling?" asks the president, "What do you mean?"

Control of data raises sovereignty issues

Processed AmI data has intelligence benefits

How is data processed?

Jurisdictional control

"Quibbling about control of the data. They say if we control the data, it's tantamount to signing their sovereignty over to us. But we've been working on a deal where we copy for them the data we collect… well, some of it, at least. Our intelligence agencies would not want us to hand over everything, and we don't have to either. We can offer the raw data to the developing countries, but certainly not the processed data. Developing countries will never know how we've processed the data, especially since we do the processing here in the United States or in the UK, i.e., outside their jurisdiction. They'll have to settle for what we give them."

"Okay, that sounds good to me. Any objections?" she asks the others who remain silent. "No? Okay, then, Jacques, it's your turn. What's the latest on the theft or whatever it was at our London office?"

Individual is in control of the technology, at least in some instances

Security audits

But before Jacques Perrier, vice president for security, can respond, the company secretary leans over and whispers something to the president. "Yes, you're right." The secretary stops the boardroom monitoring systems from recording more of the discussion on this subject.

[56] cf. O'Harrow, p. 186: "On June 1 [2004], the government granted the contract for a massive expansion of U.S. Visit to Accenture. The deal, worth up to $10 billion, will bring together an array of information and surveillance industry contracts…. In the coming years, Accenture will be helping to build sprawling computer networks and identity systems to enable the government to track foreign visitors to the United States. The company aims to create digital folders containing visitors' fingerprints, photographs, and details about their travels. The new systems will also rely on radio frequency identification and face recognition software."

Back-ups as a security measure

Alerts re anomalies

Tracking where data goes

Perrier shifts uncomfortably in his chair. "Well, as everyone here knows, we have a regular monthly audit of DMC's data processing activity. From the last audit two weeks ago, we discovered that there had been a second back-up of data immediately after the first. These back-ups are made every day. Sometimes there's a problem and a second back-up is made. It's not that unusual, but since it's not supposed to happen, we always check them out. The second back-up was anomalous too because it wasn't the whole of the database and didn't get backed up to the usual destination. In other words, we assume it was backed up locally…"

Leaving data trails

Hausmann intervenes, "By locally, you mean to another computer here in the building?"

Convenience of new technologies increases security problems

"Yes, except that none of the computers here show any evidence of having been the destination for the second back-up. That means some portable device with an optical connector was used."

"You mean like a memory stick?"

"Something like that."

Data trails

"I presume you know who made the second back-up?" asks the president.

Insiders pose the greatest security risk[57]

Despite security measures, a crime is successfully perpetrated

"Umm…uh… yes. It seems likely that it was three of my staff who were responsible for doing the regular back-ups that night. We wanted to ask them about this second back-up, but they had left on holidays a few hours after the second back-up was made. They were supposed to have returned from holidays three days ago, but they haven't reported for work and they haven't answered our calls."

The president is getting angry. "So you mean your staff have copied part of our database and walked off with it?"

Perrier is visibly squirming in his seat. "That's what it looks like."

Increasing centralisation of data poses greater risks

"And how many records do you think were copied?" she asks.

"Uh...It's bad, I'm afraid." Perrier coughed. "My guys think about 16 million."

Location implants are required to get a job

"Outrageous," says the president, slapping the table. "And why don't you know where they are? Surely you can track

[57] Keeney, et al 2005.

	them via their location implants. Everybody has to have a location implant. It's a condition of employment in our company, just like any critical infrastructure like banks, nuclear power companies, etc."
Someone is checking your data	
Undermining technologies	*"Yes, we've been checking their location data, but so far nothing," says Perrier.*
Networked AmI technologies facilitate surveillance	*"They could have been surgically removed," says Switzer. "But what about the data from the AmI systems? Have you checked the sensor networks in the homes and cars of those three employees?"*
Monitoring employees	
	"Yes," says Perrier. "Like other employees, they've agreed that we can check their home systems and we've done that. There's obviously nobody in their apartments, and their cars have been stationary since they left on holidays…"
Ubiquity of surveillance	*"And what about the surveillance systems?" asks the president. "You can't go anywhere in London without being caught by surveillance cameras hundreds of times a day."*
Monitoring	*"Yes, we've been reviewing the data from the surveillance systems too," says Perrier. "But they haven't shown up on those either. We've also been checking with the airlines and railways and car rental agencies to see where they might have gone on holidays. Now we know they left for Costa Rica, but then the trail goes cold. As Kevin has just pointed out, the developing countries don't have the kind of AmI infrastructure needed to track people, so they could really be anywhere. We've also been checking with the mobile telecom companies too, but so far, there's been no data recovered on use of their mobiles."*
Digital divide	
Data trails	
	"I don't understand how they could have got past our own security systems," says the president. "We have access control to prevent employees from unauthorised copying or manipulation of data."
Access control	
Individuals collaborate to undermine security	*"That's true," says Perrier. "The snag is that they were authorised. Quite a few employees have partial access, so if three or four with access to different bits collaborate, as these three appear to have done, they are able to get virtually full access to the data."*[58]
New technologies can be used to undermine other technologies	*"Even so," said the president, "how did they get the data outside our headquarters?"*
Hard to get in, but easy to get out – usually the	*"With today's technology, it's easy to copy vast amounts of*

[58] A Computer Security Institute study found that 70 per cent of all computer attacks came from insiders. See Schneier, Bruce, *Secrets & Lies*, p. 189.

defence is at the perimeter, rather than inside the perimeter

data in seconds onto high capacity optical storage devices no larger than a deck of playing cards, which makes them easy to conceal on the way out of the building. It's hard to break into DMC offices, but it's not hard to get out."
The president: "Are there any indications yet of what they might do with all this data?"

Drivers & criminal motives

Perrier: "No, not yet, but there are several likely possibilities, of course. They could use the identity information to commit all kinds of fraud on a huge scale without leaving any trails retraceable to them. Or they could simply sell it. There are lots of digital sites that deal in stolen data. You can easily get $100 these days for each ID.[59] *Or they could sell it to an insurance company or an intelligence agency, although we've pretty much already cornered those markets. Or they could sell it to some terrorist organisations. Or they could try to blackmail us, and we'd either have to pay up or risk the bad press we'd get if people find out just how much data we've been able to collect about them since AmI technologies became so widespread, and some of that data, as you know, has not always come from legitimate sources. Or they could blackmail victims with the knowledge they've derived from our profiles."*

Personal information is worth a lot

Blackmail

People are not aware of how pervasive AmI is becoming

"Or maybe they won't do any of those things," adds MacDonald. "Maybe they just want to make a political statement."

Public opposition to pervasiveness of AmI and/or inadequate security

"What do you mean?" asks the president.

High stakes

"They may view themselves as having a social conscience, an obligation to show how extensive our data aggregation practices have become since the introduction of AmI networks and how easy it is to pilfer the data we collect," says MacDonald. "If we were exposed, it would be a complete disaster. Among other things, it would show our clients that the profiles of our own employees were not reliable because we were not able to predict that these few bad apples were going to abscond with copies of our records."

Profit – the ultimate driver

The president snorted. "If they have 16 million records and they could get $100 for each record, I doubt they're very interested in political statements."

Obligation to inform victims

Max Court, DMC's general counsel, spoke up. "If we were exposed? Are you suggesting we should withhold information

[59] cf. Zeller, Tom Jr., "Black Market in Stolen Credit Card Data Thrives on Internet", *The New York Times*, 21 June 2005: "A 'dump', in the blunt vernacular of a relentlessly flourishing online black market, is a credit card number. And what Zo0mer is peddling is stolen account information - name, billing address, phone - for Gold Visa cards and MasterCards at $100 apiece."

about this theft from the police and those whose files have been copied?"[60]

… in the balance against the capitalist ethic

"Of course," said MacDonald. "It's obvious, isn't it? I'd hate to imagine what it would do to our share price and our plans for a listing on the Tokyo Stock Exchange."

The president took a deep breath, as if she were trying to control her temper. "You've got to find those three," she says to Perrier.

"Yes, mam. I know."

She turns to Frank Hausmann, her chief financial officer. "Okay, Frank, what's your advice about the listing on Tokyo?"

The media as watch dog

MacDonald interrupts before Hausmann could respond. "I'm sorry to interrupt again, but I was just talking to a journalist from The Financial Times. That's why I was a bit late for the start of the meeting. She rang about our intentions re the listing on Tokyo. I don't know how she knew that we were even thinking about it. I didn't confirm or deny anything. Then, she asked whether we were complying fully with the Safe Harbour Agreement. Of course, I said we were, but then she posed some very pointed questions about the security of our data. I began to wonder whether she knew about the theft of our data …"

Safe Harbour Agreement – should we assume all companies will comply?

Trade-offs
Even if data are compromised, it may not be possible to know which data have been

The buck stops at the top – the chief executive must decide

"So, Madame President, before I give my views on the Tokyo listing, I'd like to know if we are going to put out a statement about this theft. It'll make a difference about the timing," says Hausmann. "Are we going to inform those people whose records have been compromised? Are we going to tell the media?"

"We can't inform the individuals, because we don't know, at least not yet, whose records have been compromised," says Perrier.

"It's for you to decide what we should do," says MacDonald to the president.

[60] Some state governments in the US have passed legislation recently (e.g., California law SB1386, effective July 2003) that forces organisations to inform individuals whenever there has been a privacy breach, and makes organisations liable for improper use of information. In October 2005 [when this paper was prepared], a US Senate committee was considering new legislation for a Personal Data Privacy and Security Act. The bill requires that, on discovering a data breach, any agency or business entity that "uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information" notify "without unreasonable delay" any US resident whose data were subject to intrusion.

Scene 2: The Old Bailey, two years later

An AmI company ends up in court

BBC 1 news presenter: "And now we go to our reporter, Miles Davenport, who's been at the Old Bailey today, attending the trial involving the Data Mining Corporation and its directors. What's the latest, Miles? Has the jury returned with a verdict?"

Miles Davenport: "Thanks, Serena. No, the jury hasn't returned yet, but an announcement is expected in the next few minutes."

Sensationalise news

BBC presenter: "Miles, can you just recap for our viewers what this trial's been all about? And why is it so important?"

Concentration of power through concentration of AmI data

Low public awareness

Miles: "Sure, Serena. As you know, this case has had all the elements of a Jeffrey Archer thriller. It's involved high technology, secretive corporations, the world of intelligence, consumer activists, and high-level calls between Hilary Clinton, the president of the United States, and Charles Kennedy, the prime minister. Even the European Commission has got into the act.

Data mining and AmI

Linking AmI data from different sources facilitates profiling

"It all started about two years ago when The Financial Times broke a story about the theft of personal information on about 16 million people in the United States and the UK. All this personal data was held by the Data Mining Corporation, an Anglo-American conglomerate most people had never even heard of.[61] *DMC had been growing like a powerhouse through mergers and acquisitions, until it had become the world's largest data miner. It turns out that DMC had been profiling virtually everyone in the United States, Europe and many other countries around the world. They have the world's fastest and most powerful computers with billions and billions of records from all sorts of services, including governments.*[62] *DMC had been processing all these records from different sources, including the latest ambient intelligence networks, and linking them together so that it was able to build up comprehensive profiles on every one of us.*[63]

[61] cf. O'Harrow, p. 34: "Acxiom is not a household name. But as a billion-dollar player in the data industry, with details about nearly every adult in the United States, it has as much reach into American life as Pepsi or Goodyear. You may not know about Acxiom, but it knows a lot about you."

[62] cf. Solove, p. 5: "Federal, state and local governments maintain public records spanning an individual's life from birth to death. These records contain a myriad of personal details. Until recently, public records were difficult to access … But with the Internet, public records are increasingly being posted online, where anybody anywhere can easily obtain and search them." In addition, those bent on identity theft can make use of freedom of information laws. See Solove, p. 150: "The vast majority of FOIA requests are made by businesses for commercial purposes."

[63] cf. O'Harrow, p. 49: "'InfoBase Enhancement' enables Acxiom to take a single detail about a person and append, on behalf of its customers, a massive dossier. This generally happened without the individual every knowing about it."

AmI can increase the risk of ID theft

Fraud and extortion

Fall-out from data theft

Political intervention because AmI data are too valuable to allow an AmI conglomerate to go under

Recognition of value of personalisation and security enhancement from use of AmI

But AmI has a dark side too

Trust

Can data ever truly be secured?

Lack of public awareness

"Then, according to the FT, DMC discovered that someone had broken into its supercomputers and copied data on a lot of people. For a few weeks, DMC didn't say anything to anybody,[64] but then there was a big spike in the number of identity theft cases. People with credit cards were seeing all kinds of purchases on their monthly statements for stuff they hadn't bought. A lot more people and companies were reporting that they were being blackmailed with threats of releases of embarrassing information unless they paid up. The FT got wind of this big increase in credit card fraud and extortion, and was able to trace the source back to a theft of data from DMC.

"At first, DMC denied everything; then they said they wouldn't comment on it, because the theft was under police investigation. But by then, the DMC share price was plummeting on Wall Street and in London, and DMC had to call off plans for a listing on the Tokyo Stock Exchange. For a while, it looked like DMC was going bust, but the US government stepped in and propped up the company.[65] The president said that national security was involved, and they could not allow the company to go bust. People began badgering the Prime Minister about it. They had no idea just how pervasive ambient intelligence had become…"

BBC presenter: "Personalised services are great, of course; they save us lots of time. And so are the improvements in our security, knowing when we are near known criminals or people disposed to terrorism, but isn't there a dark side?"

Miles: "Well, according to civil libertarians, yes, there is. And that's partly what's been coming out in the trial of DMC. Companies like DMC hold a lot of data about all of us. And we have to trust them that our data are safe, secure and accurate. But now we know that our data are not secure.

"Questions have also been raised about the accuracy of the data. People are entitled to see their records, but most people didn't even know about DMC, let alone the fact that they had built up such extensive records on every one of us.[66] So some

[64] See Krim, Jonathan, "Consumers Not Told Of Security Breaches, Data Brokers Admit", *The Washington Post*, 14 April 2005.

[65] cf. Safire, William, "Goodbye To Privacy", *The New York Times*, 10 April 2005: "Of all the companies in the security-industrial complex, none is more dominant or acquisitive than ChoicePoint of Alpharetta, Ga. This data giant collects, stores, analyzes and sells literally billions of demographic, marketing and criminal records to police departments and government agencies that might otherwise be criticized (or de-funded) for building a national identity base to make American citizens prove they are who they say they are."

[66] Schneier, Bruce, "The Future of Surveillance", *Crypto-Gram Newsletter*, 15 October 2003: "In the U.S., data about you is not owned by you. It is owned by the person or company that collected it."

A theft amplified *Others get involved – is AmI likely to become a trade issue?*	*consumer activist groups have banded together to sue DMC for negligence, for inadequate security of their records, for not complying with the Safe Harbour Agreement between Europe and the United States. It was one of the first class action suits in UK legal history. The European Commission has got involved too. They said that the Federal Trade Commission, which administers the Safe Harbour Agreement for the US, had not been ensuring proper compliance by American companies. The Commission has also said they were taking the US to the World Trade Organisation too, because a subsidy for DMC was against its rules. It's really turned into a big mess. After this six-month trial, and thousands of pages of testimony, the end looks to be in sight."*
Other issues	*BBC presenter: "Thanks, Miles, for that recap. Weren't there some other issues that came out during the course of the trial?"*
Selling AmI data *Spamming* *Who's responsible?*	*Miles: "There certainly were, Serena. It was discovered that not only has DMC failed to protect our data, but they've actually been selling large chunks of it to governments and to other companies who in turn were using the data to spam just about everybody in the United States and here in the UK too.*[67] *DMC claimed that they couldn't be held responsible for what their clients did with the data.*
ID theft has knock-on effects	*"We also heard about fraud arising from identity theft. Some of the prosecution's witnesses said that even though their credit card companies limited losses to the first £50, fraudulent use of their cards and other personal data had knock-on effects. Credit-reporting agencies raised red flags, not only about the cards, but about the actual card holders. Some witnesses said they had been trying to get wrong information cleaned from their records for almost two years, and have yet to succeed.*[68]
AmI applications may lead to discrimination	*"Most witnesses said they've suffered from the stress involved*

[67] cf. O'Harrow, p. 135: "In 2002, the company [ChoicePoint] began allowing individuals to buy dossiers, including criminal checks, education records, and other personal details….Now everyone would soon be able to dig into the past of suspect acquaintances or employees."

[68] See Zeller, Tom Jr, "For Victims, Repairing ID Theft Can Be Grueling, " *The New York Times*, 1 Oct 2005. The story reports cases where victims have been trying to overcome the consequences of identity theft for more than two years: "Victims are still left with the unsettling realization that the keys to their inner lives as consumers, as taxpayers, as patients, as drivers and as homeowners have been picked from their pockets and distributed among thieves."

[69] cf. Solove, p. 110: "Identity theft can be a harrowing experience. According to estimates, a victim typically spends over two years and close to 200 hours to repair the damage that identity theft causes." And p. 110: "Most identity thefts remain unsolved. Research firm Gartner Inc estimates that less than 1 in 700 instances of identity theft result in a conviction."

[70] cf. O'Harrow, p. 221: "CAPPS II, shorthand for the second-generation computer-assisted passenger screening program… would piggyback on the data revolution of the 1990s, using mountains of demographic, public record, and consumer files to pluck out terrorists from the mass of people who posed

Maximising reliability, but 100 % reliability is not achievable *AmI data can help (maybe) in countering terrorism*	*in trying to recover their identities and sorting out the mess they've been put in.[69] Some said they've been stigmatised. We heard also about DMC selling their services to companies who wanted to check on prospective employees. We heard that in many instances the information was wrong, that the data coming from so many different ambient technology networks were often in conflict or didn't make any sense. DMC countered that its proprietary software contains an algorithm for comparing data from different sources to maximise reliability and its predictive capability,[70] but under intense questioning from the prosecution, they admitted they could never eliminate unreliability nor could their predictions of who might be a terrorist or criminal be 100 per cent.*
Conflicts between technologies	*"We heard about one case involving a senior civil servant whose name was put on a suspect list when it shouldn't have been. As a result of a compromised fingerprint, he couldn't even get into his own office after the fingerprint template had been disabled without his knowing it. Because he couldn't deliver an urgent file to his Minister, he became so stressed that he had to be hospitalised. His case illustrated the problem arising from different technologies no longer trusting the readings they were getting from other technologies.*
Media awareness stimulates public awareness of pervasiveness of AmI *The individual has to check*	*"As a result of the media interest in this case, many more people are now aware of how pervasive the new ambient intelligence technologies have become and how it's more important than ever that they check out what these big data aggregating companies have on them, the sources they draw on and what happens to their personal data after DMC and its competitors have processed it. If any good has come out of this case, that's surely been it."* *BBC presenter: "And the DMC directors, what's going to happen to them?"*
Escaping to an AmI-free developing country	*Miles: "We should find out after the jury comes back with the verdict. The DMC president, however, has already resigned, but she went out with a golden parachute – a severance package that included a cool $100 million – and now she's apparently living in Costa Rica."*

no threat at all. It was to be a perpetually watchful network that would electronically absorb every passenger reservation, authenticate the identity of the travellers, and then create a profile of who they are. Then it would examine that profile, instantly and relentlessly, looking for anomalies in behaviour or lifestyle that might indicate ties to terrorist groups."

[21] See O'Brien et al, p. 18: "Descriptive scenarios are based on a description of past and current trends, and may also be based on expectations of how these trends will develop in future. Normative scenarios are based on desirable developments or choices. Normative scenarios may be constructed by applying norms and values of the authors (or, hypothetically, of the society) but also by means of surveying and asking people to provide normative information."

4.2 ANALYSIS

4.2.1 Situations

The scenario has two scenes, the first of which takes place in a corporate boardroom in the year 2015, the second outside a courtroom two years later. Hence, the scenario is in the business domain.

The scenario concerns the theft (copying) of personal information held by a data aggregator (Data Mining Corporation) by three rogue employees. Theft of identity occurs now, but the difference between such crimes today and in the future is the scale of the data involved. In the future foreseen by this dark scenario, it will be possible to gather orders of magnitude more information about virtually every person in America, Europe and Japan. Our reliance on AmI will have grown immeasurably. The future is also marked by an increasing concentration in the control of personal data. Thus, the risks to individuals are much greater when something goes wrong. By the year 2015, there will have been significant technological advances, but this scenario posits that there will have been little evolution in business ethics, management practices and public awareness.

4.2.2 AmI technologies and devices

The scenario makes reference to several AmI or AmI-related technologies, including

- biometrics, including a fingerprint reader and iris scanner, which serve security purposes in admitting entrance to a restricted area (the boardroom) by only those authorised to enter,
- networked sensors/actuators, which are linked to the fingerprint reader and iris scanner and which activate the lighting and air conditioning in the boardroom based on the known preferences of those entering the boardroom. To deal with several competing individual preferences, the actuators calculate the mid-points of those in the room,
- wafer-thin displays which can switch from textual information (the corporate management committee's agenda) to visual imagery from surveillance cameras which, at the same time, display the reference person's location co-ordinates in real-time,
- voice-activated access to an intelligent environment as shown in the board room meeting,
- surveillance technologies which management can use to monitor employees, both in the office and outside (e.g., in their homes or cars). Surveillance technologies include video cameras, key logging software, location implants, biometrics and networked sensors,
- location implants and location-reporting devices, which employees are obliged to bear (e.g., implants) or wear as a condition of employment,
- machine-learning technologies which analyse past behaviour and preferences in order to predict needs and to personalise services,
- networked RFIDs, sensors and actuators for gathering data about people and the products they have or services they use,
- fourth generation mobile phones, which combine today's PDA capabilities with third generation mobile technology (and much else).

4.2.3 AmI applications

The AmI technologies referenced in the scenario are used in various applications, including

- security – Biometrics are used for admission to restricted areas such as the corporate boardroom as well as the DMC headquarters building. Access control technologies (e.g., biometrics) are used to govern who can have access or make changes to DMC's databases,
- surveillance – The president and his corporate colleagues are able to watch MacDonald in his office and on his way to the boardroom. References are made to surveillance of employees outside the office as well. Sensors in homes and cars are networked and provide information to DMC senior management as to whether an employee is at home or in his or her car,
- immigration control – AmI technologies enable the building up of much more comprehensive profiles of individuals, so much so that prospective visitors or immigrants from countries without AmI networks may not in future be admitted to the developed countries because, in the absence of AmI networks in their own countries, there is not enough information to assess whether the candidate is trustworthy or a security risk,
- personalisation of services – AmI is used for personalisation of services such as lighting and air conditioning set to one's preferences as well as services provided by products and services such as PDAs and mobile phones. Personalisation of services also leads to time-savings since AmI networks can, for example, monitor the status of one's consumables (such as food and drink) and place orders with the supermarket as necessary,
- targeted marketing – With more detailed data on consumers, retailers, media conglomerates and others are able to engage in targeted marketing with greater precision,
- improved profiling – Insurance companies and credit-reporting agencies are able to assess individuals against insurable risks and creditworthiness. While this is good for the insurance companies and credit-reporting agencies, it may not be so good for individuals who may find it harder to get insurance or credit,
- counter-terrorism and policing – With more detailed data on individuals, intelligence agencies and police forces are better able to assess and counter terrorist risks and combat crime,
- critical infrastructure protection – Although protection of critical infrastructure is only mentioned in passing in the scenario, AmI provides the means to better protect critical infrastructure (including the AmI networks themselves) from intruders (but not necessarily insiders) bent on damaging or undermining those networks.
- fourth generation mobile phones, which combine today's PDA capabilities with third generation mobile technology (and much else).

While several positive, socially useful applications are alluded to, there are some negative applications too. Among them:

- spamming – The huge increase in data about individuals facilitates more precision in spamming and targeted marketing.
- fraud – Similarly, the opportunities for fraud are improved because more detailed information is available to criminals.
- blackmail – With more detailed information, criminals are in a stronger position to

blackmail those whose data they hold.
- discrimination – With more detailed information, insurers are able to discriminate against some people who pose higher risks than others. Conversely, the lack of information on some people (e.g., those from developing countries) means that they too could suffer discrimination, i.e., if they don't have an adequate data trail, they may not be admitted to developed countries.
- terrorism – Terrorists have more opportunities and better information to impersonate others when they have access to the detailed data on individuals provided through AmI networks.

4.2.4 Drivers

The scenario hinges on the theft of data from DMC and the consequences of that theft. The drivers at work here can largely be derived from the motives and needs of the principal characters or groups of characters.

DMC has aspired to be the leader in its market, something it has achieved. DMC's success can be attributed to at least two or three key factors. One is that it has been able to aggregate more data on individuals than any other company. A principal source of these data is the AmI networks that are able to generate far more information than ever before on individuals, their behaviours, habits, contacts, comings and goings, purchases, etc. A second success factor is that DMC has developed an algorithm for sifting through and processing all this data so that it is able to sell its products and services to a wide range of clients. A third factor could be the quality and vision of its management, without whose leadership (and their business plan) it would not have been able to achieve such success.

For the management, one could conclude that they are primarily driven by the profit motive and a desire for scale (i.e., to be the market leader and, presumably, to swallow or overwhelm competitors) and to create a situation where their clients are dependent on DMC services and products.

A second driver must be market demand, i.e., there are many companies and governmental agencies who want the processed data which DMC has been supplying.

A third driver, not so dissimilar from the first, is that the data thieves are also impelled by the profit motive. In their case, however, one could conclude that they see an opportunity to make more money more quickly by copying files from the DMC database and selling it to fraudsters. Before the spike in reported instances of identity theft, Perrier, DMC's vice president of security, speculates what the data thieves might do with the data, which point to drivers. He says the data thieves could sell the data to an insurance company or intelligence agency or to a terrorist organisation or blackmail DMC and/or the individuals whose data they have copied (i.e., the driver is to make money). MacDonald speculates that the data thieves might have committed their crime in the public interest – i.e., to make people aware of how much information DMC was collecting on them through the aggregation of data from AmI networks and to make people aware just how ill-protected and insecure their data are.

A fourth driver is respect for the law. This is indicated when DMC's general counsel expresses some disbelief at the suggestion that DMC should cover up the data theft from

both the police and those whose files have been copied. As he makes only one intervention in Scene 1, we might not want to attach too much importance to this driver. In Scene 2, however, the court case indicates that respect for and redress through the law is a much stronger driver. The lawsuit against DMC is brought by consumer activists seeking restitution (=a fifth driver) for the aggravation caused to them through DMC's negligence.

Yet another driver can also be identified, i.e., the media's desire for a good story which has the benefit of raising public awareness about the pervasiveness of AmI and AmI's benefits (e.g., greater convenience through personalisation of services and improved security) as well as possible risks (encroachment on privacy, exploitation by terrorists, criminals, intelligence agencies, insurance companies, etc.).

4.2.5 Issues

The scenario raises several issues:

Digital divide

The developed countries have AmI networks and the developing countries don't. There is a risk that this will lead to discrimination against developing countries because the intelligence agencies and immigration authorities may not admit visitors and emigrants from those countries because they do not have the detailed information on individuals from those countries that they do on individuals from developed countries and, consequently, are not able to assess whether individuals from developing countries are a security risk.

On the other hand, DMC executives see an opportunity to set up AmI networks in developing countries which could overcome the concerns of the intelligence agencies and immigration authorities, but potentially leads to another form of discrimination whereby the data arising from the AmI networks are processed by DMC in the US. A sop would be given to the developing countries, i.e., the raw data, but the real juice is in the processing and exploitation of the data. Switzer mentions the fears of developing countries that they would effectively be transferring their sovereignty to the developed countries (if not to DMC).

Concentration of power

DMC is the clear market leader in the aggregation and processing of AmI-generated data. Its clients include a wide range of powerful clients – the media, retailers, credit-reporting agencies, immigration authorities, intelligence agencies, etc. When there is a risk that DMC might collapse as a result of the fall-out from the theft, the US government steps in to prop up the company on the grounds that, for security reasons, it cannot permit the collapse. This in turn leads to a dispute between the US and the EU as the EU claims that a subsidy would be violating WTO rules.

Lack of public awareness

Despite the convenience of the increasing personalisation of services and the enhancements in security that AmI has made possible, most people have not

comprehended just how pervasive AmI has become, nor of the scale and volume of data being generated about them by AmI networks. Everything produced will have an AmI-networked microchip.

Most people are willing to trade some of their privacy for better security. The scenario suggests that terrorism has become sufficiently serious that the intelligence agencies and immigration authorities are becoming unwilling to admit foreigners unless they have detailed information on each individual. Similarly, DMC employees seem willing to have location implants and surveillance equipment installed not only in their offices but in their homes and cars. Probably, they see this as beneficial in security terms.

In the scenario, public awareness is increased as a result of the investigative reporting and media coverage of the theft of data from DMC, the resulting trial and the high-level political intervention. Identity theft is not, of course, a new crime, but what is new about the DMC case is just how extensive are the data from AmI networks compiled and processed by DMC.

The illusion of security

It is ironic that DMC and its directors face a class action lawsuit on the grounds that they were negligent in securing personal data. It would seem DMC has many security measures to do just that. They have installed surveillance equipment, biometrics, key-logging software and other access control measures to protect the data they hold. One of the vice presidents says it is hard to get into DMC headquarters. But the question is: have DMC executives done enough? Did they think their profiling of their own employees was sufficiently watertight so that they did not need to fear theft by insiders? Maybe. We are told that it was hard to get into DMC offices, but not hard to get out. Also, the president seems surprised by a breach in DMC security. Furthermore, they don't know which specific files have been copied, only that about 16 million were copied. DMC's security defences seem primarily aimed at keeping people out, from preventing breaches at its perimeter. The company seemed rather less focussed on the enemy within, hence the three employees (who had authorised access to the data) were able to copy the files and exit the premises without having been challenged. Further it seems relatively easy for them to have removed their location implants and to have disappeared without a trace.

Differences in legal regimes

In the first scene, MacDonald says he was questioned by a reporter about whether DMC was complying fully with the Safe Harbour Agreement. At this time [2005], there remains a difference between the privacy and data protection requirements in Europe and those in the United States. The Safe Harbour Agreement was supposed to ameliorate those differences, but questions have frequently been raised about its effectiveness and whether (some) companies are complying with the Agreement even if they say they are. The scenario suggests that DMC has largely ignored the Safe Harbour Agreement as it has sold data to a wide range of clients, including government agencies.

Honesty and trust

Given the lack of awareness of most people about the extensive records held by DMC,

the issue of trust is not directly raised, but nevertheless it is an issue whenever a third party holds personal data, especially a lot of data as in the case of DMC. One would think that a data aggregator, processor and reseller like DMC would have some obligation to inform people whenever it sells data to others or takes over another company with personal data records. But this has not occurred. One could assume that some DMC clients such as the intelligence agencies and immigration authorities are content that individuals are *not* informed about what information DMC has on them.

In Scene 1, we do not know the president's decision about whether to inform the police and individuals about the theft. Even so, MacDonald, the vice president in charge of media relations, does not hesitate in expressing the view that they should *not* inform the police or individuals. In any event, it seems DMC doesn't know (yet) whose records have been copied. In the US, as mentioned in the endnote to Max Court's comment, California and a number of other states have strict laws requiring that companies *do* inform individuals when their data have been stolen or compromised – but that does not mean that they will. Compliance will depend as much on corporate culture and, especially, ethics as on legal deterrents. Senior managers must be seen to be fully compliant and to instil a culture of good corporate citizenship.

4.2.6 Legal synopsis

Disparities in the legal systems and applicable law

In an AmI world, the globalisation of commercial activities will be even greater than today. The question arises how to resolve the problem that different data protection standards apply in different legal regimes. Currently, there are certain legal boundaries for transmitting data from the EU to third countries not affording adequate legal protection comparable to that afforded by the Data Protection Directive. The adequate protection may be ensured by national standards in force in the given country, as well as by compliance with international instruments such as the Safe Harbour Agreement. This agreement provides a solution to some of the disparities. Still, questions remain on the effective enforcement of such provisions. The issue of exchanging data with countries that do not provide adequate protection may cause problems. The Data Protection Directive provides exceptions to the prohibition of exchanging data with third countries, provided that some strict requirements are fulfilled. Still, as we see from the scenario, compliance with the legal provisions is a problem.

The differences in the legal regimes also leads to the question of which law shall be applicable to which data processor, as well as to other situations. Current EU legislation is based on the "place of processing" as a determining criterion in choice of the applicable law. It would be difficult, however, to determine where the processing was carried out and easy for the data processor to move his place of processing outside the EU. In such a situation, the data subject would lose the protection of European law, and possibly also of its own national legislation. Another criterion to determine the applicable law seems desirable.

Privacy

It is already increasingly difficult to create the right balance between the legitimate interests of enterprises, security requirements and the protection of the private sphere of

the employees. Currently, there is no harmonisation on rules relating to monitoring of employees (and protection of their privacy).

Digital divide and standardisation

In order for AmI to function beyond borders, different regions or countries need to use technologies that interoperate. Further harmonisation of standards will be needed, both within the EU and at international level. It must be remembered, however, that some countries will not be able to afford to comply with the standards created in developed countries. This is already a huge problem. Solutions to overcome such disproportionalities should be envisaged.

Trading in data and data laundering

Data collection and trading of data raises the problem of ensuring that data are collected from legitimate sources, avoiding data laundering and abuse of the data. Similar obligations should be imposed on enterprises like those dealing with money laundering. Companies should be obliged to check where the transferred data comes from.

Intellectual Property Rights

The current Intellectual Property Rights system provides extensive protection for the author of databases. In an AmI world, information holders, database authors, service suppliers would have to co-operate promptly and at reasonable cost. It seems that the current systems cannot provide solutions to address such needs, since the system demands, for example, consent from the data authors. This allows the rights holders to impose high prices and makes it possible to conclude exclusive contracts.

Criminal liability

The Cybercrime Convention provides for a common definition of a number of computer related crimes. The legal provisions currently in force require a sufficient degree of intent, which can cause certain problems. The criminal liability of legal persons is, however, specifically foreseen.

4.3 CONCLUSIONS

The principal conclusion we draw from this dark scenario and its analysis is that, although we can expect amazing advances in the development and deployment of ambient technologies, there is a risk that corporate ethics in the year 2015 will not be so different from those prevalent in the year 2005, which is to say that some companies will be good corporate citizens and some won't. Similarly, some companies will have rogue employees just as they do today who are capable of undermining the efficiency and credibility of new data processing algorithms. A principal difference between today's world and that depicted in the year 2015 could be that security concerns about terrorism and anti-social behaviour will be such that unless individuals have really detailed profiles compiled from data from AmI networks, they may be barred from entering a developed country. Also, while people may welcome the convenience from personalisation of services and the ubiquity of surveillance technologies, they may be

lulled into a false sense of security.

In view of the advances in surveillance technologies, biometrics and fourth-generation mobile systems, the AmI community, policy-makers and society must be alert to possible abuses of the technology. Consequently, it is important to build in safeguards that minimise the risks, even though it must be recognised that the risks can never be completely eliminated, no matter how strong and comprehensive the legislative and regulatory measures are.

5 DARK SCENARIO 4: RISK SOCIETY

5.1 THE SCENARIO SCRIPT

Introduction

In the TV studios of an early morning news and variety show, a reporter/presenter is interviewing people who have made the news.

"Good morning ladies and gentlemen and thank you for joining us here on The Breakfast Show. Our guests today include a researcher in the Antarctic and the winner of last month's reality gardening show. We'll also have the latest traffic forecast across the city which appears to be normal considering yesterday's chaos. The CO^2 pollution levels is below the threshold so all cars are allowed to enter the city centre. First though we are pleased to welcome to the studio Markos, an MEP and one of the founding members of APPAG."

Scene 1: The Anti-Personalised-Profiling Action Group (APPAG)

Breakfast Show Presenter: "Markos, thank you for taking the time to join us today. Tell us about APPAG and how it came about."

Different levels of profiling (aggregate vs personalised)

Risks of personalised profiling

People are not aware how much is known about them or what digital traces they leave behind

"First off, Alexandra, I'd like to thank you for inviting me. APPAG is something I feel quite strongly about and I'm glad to have the opportunity to share it with your viewers. The initials stand for Anti-Personalised-Profiling Action Group. I would like to stress right from the beginning that we are not against aggregated profiling per se. In fact, I was an early adopter of the 'always-on' movement some 10 years ago during the broadband Internet/mobile convergence era. I am also used to being watched and surveyed at all times because of my position as an MEP. But I think a lot of people simply do not realise how much personal information they are constantly giving out."[71] *APPAG wants to raise public awareness about this issue and wants to warn people that personalised profiling is simply too risky. I joined APPAG after some bad experiences."*

"What kind of bad experiences?"

Being deprived having

"First of all, during our last holiday, my wife and I discovered that we did not have access to the same information and

[71] Tuohey, Jasey, "Government Uses Color Laser Printer Technology to Track Documents. Practice embeds hidden, traceable data in every page printed", 22 November 2004. http://www.pcworld.com/news/article/0,aid,118664,00.asp. See also Jardin, Xeni, "Your Identity, Open to All", *Wired News*, 6 May 2005. http://www.wired.com/news/privacy/0,1848,67407,00.html

access to certain services (unfair – not everyone being treated equally) *Profiling exclusivity* *Dependence*	*services as other hotel guests. For example, there was a jazz concert in town during sunset but we did not get any information about it. We only found out the next day. I was really angry because my avatar knows I like such events. Also, the excursion to the old Roman ruins was already fully booked. We could only participate when paying a premium. This is so unfair. And do you know why? Just because the company that has the profiling exclusivity on our family recently merged with another company. Because we did not opt in to their new travelling module, they ignored the travelling preferences of my avatar. And then suddenly, you realise how dependent you have become on these things."* *"But is that solved now?"*
The hassle of switching off	*"Yes, but … it set me thinking. What happens if you decide not to do it? I began to make a point of switching off my AmI sensors in public places so that my preferences could not be revealed and monitored. I'll leave them on in the home where I control the environment, or at work where there are confidentiality clauses protecting us but the moment I step outside I switch them off. A cumbersome procedure, a real hassle, but it can be done. The downside is that I now find myself missing out on announcements – including the emergencies – or special promotions that I would have liked to take advantage of. Recently, I was in the airport where I actually found that I was banned from the frequent flyers' lounge because their sensors objected to my sensors opting out! Even though I showed them my card, they still wouldn't let me in. Can you believe that? Why should I be denied entry? Now I can see that if I have my AmI sensors off at the airport, there's a distinct risk that I'll be stopped and searched and maybe miss my flight."* *"But why would you want to switch …?"*
Lack of freedom in decision making *Personalised profiling.* http://www.theisland-themovie.com/	*"Because I value my privacy. I think a lot of people simply do not realise how much personal information they are constantly giving out. What I object to is the personal nature of this profiling. Personalised profiling leads to a lack of freedom in making a decision. Have you heard about the companies with plans to 'personalise' their self-service restaurants based on their customers' medical history? Imagine, you would like to have a steak but they give you a salad instead … And what if insurance companies get involved and start raising your premium because they found out that you are not doing a lot of physical exercise?*
Surveillance	*"I understand companies collect anonymous information to better serve their clients or for particular marketing purposes*

Free choice?

although this also has caveats that one should look into. But it's the idea that you are being personally profiled wherever you go that really concerns me. It is the amount, quality and accuracy of data related to you that is generated and collected and archived for eternity that makes me shiver. How do you know the choice proposed by an avatar is a consequence of your preferences or simply the imposition of a commercial agreement?"

"What do you propose then?"

Anonymity

Anonymity profiling

"Some believe that anonymity is the solution but I am not sure about that. The system needs your identity and you must give it in order to get access to the services. I think people should stop giving their data away for profiling purposes because once the system has them, the profile is built, improved, linked, added with other information.
And you know what the worst thing is? Even if you refuse any profiling, and you want to act as if you are anonymous, you fall within a profiled category called "the anonymous". It is even one of the best profiled categories …! You just can't escape it any more."

"You also say that we need to be careful when transferring human judgement and decision-making to computers."

Quick profiling and decision making on limited amount of data

Rectification procedure

"Yes, to give an example, a good friend was erroneously placed on a tourism black list. These lists are used by the major hotel chains to identify known trouble-makers, people with bad debt or whatever the case may be. If you present yourself at a hotel reception desk without an advance reservation, the big hotel chains will run a quick profile on you. The problem is that that it takes time to go through the massive amount of data. As a result, an early warning system is set-up that already gives suggestions after only five per cent of the data has been processed. Experienced hotel staff knows how to deal with such preliminary profiles but in this case the lady in question was refused a hotel room. The situation was not rectified until the following day. In the meantime, my friend had to spend the night in a hotel that was dirty, noisy, dangerous and twice as expensive but it was the only one that accepted her cash and did not require the result of the standard profiling application. On top of this, her suitcase was stolen there. Who do you think is liable for that? Moreover, there will probably always be a record of this somewhere, even if it was cleared up the next day, and you never know if something similar might happen again. Not a very nice prospect."

"Tell us about what APPAG proposes?"

Personal data – legal framework	*"Well, one of the fundamental areas we want to work on is the legal framework. Though the data protection act covers personal data, we feel that there is a grey area about what really constitutes personal data and under what circumstances data collection is legal. I would argue that many of your preferences and lifestyle choices are, in fact, personal data.*
Awareness raising	*"Furthermore, as I said earlier, we want to raise public awareness about these issues. Many people do not know what information is being collected and do not even know they have the right to opt out. This must change."*

Scene 2: AmI divides

"We now go live to New York where we are joined by Dr. Anthony Lazlo, a leading environmental scientist and pioneer of AmI for environmental protection who is very critical of current environmental protection programs. Good morning, Anthony."

Environmental protection *Policy context*	*"Good morning, Alexandra, and thank you for the invitation to appear on your programme. I want to show you and your audience that our society is not making full use of the potential of environmental monitoring technologies but also that policy-makers need to understand that intelligent devices and intelligent agents alone are not going to solve the problem. The future simulations we will project are based on the widespread use of AmI sensors throughout Antarctica which have been collecting all sorts of information during the last 10 years."*
	"Can you tell us more in detail what you mean, Anthony?"
Environmental sensors *Smart dust* *Hazards and disasters*	*"Of course, and I will show it to your audience. Have a look at these images live from Antarctica, which has one of the harshest climates on earth. Within the GCP – the Global Conservation Project – we have spread thousands of sensors in the environment to constantly monitor climate change.*[72] *That is because the costs of these tiny sensors – they are actually like smart dust*[73] *– have gone down drastically, although it is still very expensive to cover such a big landmass, especially under inhospitable conditions. But it is necessary, as rising sea levels have caused much destruction in the last few years. Look also at the projected graph with the information we receive on the water temperature, sea level, air pollution, etc. Similar smart monitoring projects in sensitive zones all over the world would help us seriously in combating environmental hazards and disasters, and could save many, many lives."*

[72] For instance, Michahelles, F., et al., 2003.
[73] For instance, Smart Dust project, http://robotics.eecs.berkeley.edu/~pister/SmartDust/

"So why are we not doing it then?"

Political priorities

"Because there is not enough money for it. I mean, there is little commercial interest in this, so it needs to come from public funding, but political and governmental priorities are elsewhere. Now look at these images from a very different place, the hot and dry Saharan desert. These images came from a film shot by a camera crew that travelled recently to the region. Here too, we can see environmental destruction. But here we do not have the technology to enable us to act quickly and remotely. But let me be clear about this. I'm not talking about just environmental issues. AmI technologies could have life-saving potential – if we were able to monitor the spread of certain viruses, for example, we could target immunisation programmes more effectively and stand a better chance of eradicating diseases. Instead medics working in the field here do not even have the latest 4G terminals with language translation and direct connection to medical laboratories."

"So you're saying more public money is needed?"

Ami to benefit all

"Yes, but not only that. We want to draw attention to the fact that although in some places we have been able to use this technology and harness its full capabilities, there are many other regions in the world which could greatly benefit but which do not have the funds to make the necessary investment. That is not fair. It should not be like that."

"Thanks, Anthony, for drawing our attention to this issue. Any last messages?"

Socio-economic aspects

"Yes. It is not only about money nor only about technology. You can invest lots of money in technology implementations but if no political action is taken or if people and companies are not willing to change certain behaviours, then we are going the wrong way. All the money in the world would not be able to change that nor the most fantastic technologies."

"Unfortunately we have to leave it there, Anthony. We now go to Iris for the most recent traffic information."

Scene 3: Public life disrupted by virus attack

Context of interview 3

Public monitoring

"The traffic situation downtown is currently heavy but stable. The communication backbone seems to be coping today with the heavy traffic of all the machine-to-machine messages that maintain increased traffic throughput. Pollution levels are steady, the emergency response rate is up by a point, crime-monitoring is at alert level yellow, and the accident rate is close to zero. A distinct improvement compared to the situation at the

same time yesterday. But let's talk to Peter, our correspondent at the city traffic office, for the latest news on yesterday's chaos."

"Good morning, Peter. Tell us what happened yesterday. Was it a virus attack?"

Virus attack

City traffic chaos: dependability of traffic systems

"Yes, it was. The city's intelligent traffic system went completely mad and the resulting traffic chaos was the worst we've seen in more than 15 years. Traffic lights kept on alternating every five seconds at random, for almost an hour. Cars were let into the city centre without being automatically charged the congestion toll thus contributing to the general chaos; road works were wrongly announced creating queues of angry drivers complaining to technical staff and buses did not stop at (digital) requests. According to a traffic official, the centre's main server was attacked by a digital virus. Initially, the self-repairing anti-virus software was able to counter the attack and in order to completely eradicate the hybrid virus (or multipartite virus), the software had to search for, identify and download software updates. Unfortunately, an unknown Trojan was able to briefly take control of the traffic management system. Emergency back-up systems were able to restore control after 45 minutes, but the impact on the city traffic lasted for many more hours."

"Peter, what did traffic administration say about it? It was obviously a serious security breach."

Terrorist attack?

Type of virus

"Well, during the crisis, it seems their primary goal was to restore the situation back to normal as soon as possible. Once that was accomplished, they started asking questions about the attack. Who perpetrated it? What was their objective? Was it a diversion for other types of attacks, such as crime, robbery, etc.? They are seriously considering the possibility that this may have been a malicious terrorist attack[74] and are trying to find the missing links. Their specialists looked into the hybrid virus and the Trojan, and after analysis, they declared this morning that they were not dealing with a new-generation virus. The consequences would have been worse if this had been an attack using novel mutant type worms."

"Is there a longer term impact of the attack?"

Data loss

Self-learning systems lose their intelligence

"Well, city officials aren't saying anything officially, but there's a rumour goes that the virus also caused partial loss of traffic data. That would mean that the traffic system has lost its intelligence and that it has to learn again to optimise traffic

[74] For instance, Schneier, B., 2004.

intervention measures. It could take up to two or three months, but again, this is an unconfirmed report.

"Officially, the city traffic experts say only the obvious, that security is critical in AmI environments like the traffic management system and that "we" need to reduce the risks relating to the upgrading, maintenance and interoperability of such systems. Is that another way of saying they want more money? Who knows? Back to you, Iris."

"Next, our events correspondent, Didi, is at the scene of yesterday's rock concert, where security fears prompted the evacuation of almost 50,000 people. Fans are now demanding their money back as it emerges mishaps with the technology used by event organisers may have been to blame.

Scene 4: AmI system aided mass risk management

"Here's Didi with our special report on the story." [Voiceover of report]

AmI crowd management

Edibles, tiny chips you swallow which transmit an (anonymous) identity. Can also be used as valid tickets.[75]
Personal & Disposable Wrist Communicators

Pre-prepared profile:

Concert mode allows everyone in the venue to interconnect, but it also gives event organisers a direct channel of communication in case of emergency.

"Incidents in the past with big crowds led to the development of crowd management strategies supported by AmI technologies.[76] *AmI has proved to be effective in facilitating intelligent communication among infrastructural elements (AmI sensors), event organisers, security managers and members of the crowd. Through the use of Edibles, Personal Wrist Communicators (PWC) and Disposable Wrist Communicators (DWC), crowds and individual movements are monitored continuously so that any incidents are noticed immediately.*[77] *This time, however, the system did not function properly. The concert hall was evacuated completely because panic arose for no reason at all; it appeared afterwards, although all identification devices were automatically switched to 'Concert' mode.*

"Last night, not everyone made the switch to 'Concert' mode. Early generation devices, very popular among the teenagers, were not sold with pre-prepared profiles and users of these devices had to create the profile manually; some did not do so. Other users simply did not download the concert profile as it was sucking up resources of their personal AmI devices. Thus, their AmI devices did not function properly. On the other hand, people with implants, through their intelligent

[75] Gilbert, Alorie, "RFID chips in humans get green light. FDA gives approval for use in patients", Silicon.com, 14 October 2004.
http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39124983,00.htm
[76] Hogan, Jenny, "Smart software linked to CCTV can spot dubious behaviour", New Scientist.com, 11 July 2003. http://www.newscientist.com/article.ns?id=dn3918
[77] Upton, Mick, "Casual Rock Concert Events", June 2005.
http://www.crowddynamics.com/Main/Concert risks.htm

proxies, were able to effortlessly negotiate, check and download the appropriate concert profiles. Also, people who had bought their tickets from ticket touts, habitually labelled 'clones', tried to mask their identity and assume the name corresponding to the ticket.

Location-specific information

Security measures

"The concert began with a great performance from The Tumbling Rocks. Suddenly people say they heard a loud bang. Witnesses at the scene described hearing something that sounded like an explosion. Others assumed this was just a part of The Rocks' act. Those members of the audience with personal devices running the concert profile instantly received 'no-panic' messages; others were not notified at all. The security resources control centre received various messages from the audience as well as from the arena AmI sensors and the ground patrol which immediately approached the scene. The first priority of the ground patrol was to arrest all 'clones' as a matter of precaution. In addition, a special report was sent to all emergency services that were on stand-by including the status of the AmI sensors in the area (quantity and quality parameters) and the list of who was in the audience and of their personal AmI devices. An in-depth identification analysis of all clones was also initiated.

Interaction AmI and mass behaviour

"Parts of the audience started moving away from the affected spot despite the fact that there was no cause for concern. Crowd behaviour monitoring devices detected this panic movement and the AmI system automatically initiated the evacuation plan for this part of the arena without alarming others. Then, confusion occurred as some people took decisions in spite of AmI recommendations while others were unaware of any abnormal occurrence. It was finally decided to evacuate the whole arena and the appropriate plan was put in motion. Apart from a few people being lightly injured and some 'clones' being arrested, the evacuation plans were executed perfectly. The snag was that everyone felt disappointed and cheated that the concert had to be abandoned. Naturally, people want their money back."

Back in the studio, Alexandra thanks Didi for the report and passes on to her next guest, the winner of last month's reality gardening show. Life goes on even in AmI space.

5.2 ANALYSIS

5.2.1 Situations

This scenario is intended to explore the implications of AmI technologies on a global scale and to consider risks for society as a whole. It highlights possible problems related to critical infrastructures, security and dependability. The scenario is composed of four interviews:

- the first deals with the application of personalised profiling in public spaces and voluntary exclusion from AmI services as a result of negative experiences (invasions of privacy, profiling, annoyance, etc.),
- the second tackles the issue of the digital divide,
- the third shows how AmI vulnerabilities and our dependence on critical infrastructure might affect public life,
- the last concerns application of AmI technologies for crowd management.

Scene 1:
In this interview, a member of the Anti-Personalised-Profiling Action Group stresses the risks related to personalised profiling in public spaces as opposed to the milder risks as a result of aggregated profiling and underlines the lack of awareness from users and the lack of transparency from providers. Some critical situations are described:

- being deprived of access to certain services or unable to get your leisure of choice,
- the lack of freedom in decision-making,
- avoiding anonymity as it is a profiling category in itself,
- the difficulty in recovering a “stable” (legitimate) situation as a consequence of transferring human judgment and decision-making to computers.

Scene 2:
AmI technologies may contribute to improving the climate sciences,[78] by

- enhancing access to and integrating available information from sources such as electronic journals, satellite data, etc.,
- including researchers in the global geo-science community and by enhancing virtual collaborations.

In addition, AmI technologies can help create a better understanding of climate change by enabling continuous monitoring and serving as an effective tool in reducing climate change impacts, such as natural disasters.[79] However, AmI applications, installation and maintenance may have a prohibitive cost.

- The issue of digital divide at global level is also addressed. The dark side has two manifestations: Not every country can benefit in same way from AmI technologies, although the impacts are global.
- AmI technologies as such will not solve the digital divide problem. Effective distribution of organisational responsibilities and policy measures are needed as well.

[78] Gettleman, 2003.
[79] Müller, 2002.

Scene 3:
This scene aims at raising awareness of our dependence on the infrastructure and the required level of security – a critical issue in AmI environments. Indeed, new technologies bring new vulnerabilities (as shown in the weakness of the self-repairing anti-virus software). When they are exploited, the consequences (e.g., the traffic chaos caused by usurping control of the traffic management system) may be significant. A post-crisis analysis underlines the impacts and damages (e.g., loss of data) caused by this digital attack and the subsequent actions to be performed (e.g., application of learned lessons). With the complexity of the AmI environment and the increasing dependence on AmI-enabled services, security of systems becomes critical. They need to be protected from terrorists, common law criminals, hackers and software bugs.

Scene 4:
The last interview recounts how continuous AmI monitoring of specific large public spaces such as a stadium and personalised communication to thousands of individuals may help risk management by establishing a direct channel of communication between people and event organisers in an emergency. The expected benefits are important, but the practice reveals some problems, such as inappropriate communication and confusion in the audience mainly due to lack of trust in the AmI suggestions. Even if the AmI system works as anticipated, the result might generate more inconvenience than benefit. In view of their ubiquity, AmI technologies and devices can help in risk management and crowd control, but challenges to their utility need to be pre-empted.

5.2.2 AmI technologies and devices

The scenario makes reference to several AmI or AmI-related technologies, including

- sensors
  - tiny sensors (actually, smart dust) embedded in the environment with networking capabilities for monitoring climate change;
  - positioning
- intelligent algorithms
  - data mining (for providing personalised information such as about a jazz concert to hotel guests or for personalising self-service in a restaurant)
  - self-repairing algorithms, e.g., to optimise emergency intervention in traffic management
  - traffic routing
  - language translation
- wireless and wireline communications networks enabling interworking of heterogeneous devices, including networked sensors, computers and diverse personal devices.

5.2.3 Applications

The AmI technologies referenced in the scenario are used in various applications, including

- personalisation of services – AmI profiling aims at providing well-being and helping users in their everyday life. Several examples can be found in this scenario, such as hotel-restaurant services, establishment of a specific channel for emergency, etc.
- environmental monitoring – AmI applications will enable continuous monitoring, even under hostile conditions, and provide information/data in order to help solve

global problems.

- traffic, emergency and crowd management – Because AmI technologies can provide more detailed, individualised, real-time location data from networked sensors, intelligent systems can be implemented for crowd configuration, pro-active and adaptive evacuation and incident notification. The key technologies or devices in such management applications include
  - profiling – personalised or for a group – which can improve the responsiveness of the AmI environment,
  - avatars used to encapsulate user experiences, preferences and wants,
  - disposable (e.g., edible) communication hardware,
  - 4G terminals enabling language translation among many other services.
- self-repairing anti-virus applications – On-line AmI technology makes it is possible to design self-learning intelligent systems.
- security measures – AmI has the capability to support effective decision making.

Because new technologies bring new vulnerabilities, some negative applications may arise, including

- propagation of viruses – Inherent in the implementation of any AmI environment is the interoperability of different technologies. That interoperability requires metadata, and we could expect such metadata to be exploited or attacked by a new generation of powerful viruses, mutant worms that can adapt to network and device heterogeneity to spread and disrupt different AmI devices including back-up systems,
- fraudulent gathering of personal information and profiles,
- exclusion of people by placing them on a black list based on automatically gathered information.

5.2.4 Drivers

The four scenes in this scenario are driven by several drivers, of which the following are the most important:

Individual and social concerns about the deterioration of the environment

As a consequence of this prevalent concern, individuals, scientists, social groups and others have begun using AmI to monitor changes in the Antarctic environment. It is simply beneficial to all to facilitate the use of such advanced technology everywhere.

The desire to control others and the external world

This driver makes use of technologies enabling monitoring, profiling and tracing. These technologies are based on an intensive collection of several types of data (location data, personal data, etc.). Generally, users are not aware of the collection processes. Consequently, two subsequent issues rise: difficulty in protecting personal data and loss of control.

The belief in technological progress

This driver is associated with the willingness of individual citizens and consumers to use and adapt their behaviour to the technological possibilities of AmI. Acceptance and

demand for AmI products and services will drive the development and provision of applications. Consumer understanding of the benefits of AmI applications and the effectiveness of human-machine interfaces are relevant issues.

Costs

The drive towards cost saving could give a boost to the implementation of AmI but maintenance and updating could be more costly than expected. Therefore, costs may be the source of dark situations involving the digital divide between countries and the categorisation of users.

The desire to live a private life

The right to privacy is an important driver as well as a key issue, particularly as it concerns the protection of personal data from exploitation (i.e., identity theft). Privacy is likely to play a key part in user acceptability of AmI applications and services. It will drive people to select (or not) products or services that offer privacy protection; it also forces manufacturers and service providers to build into their products and services privacy-enhancing technologies.

5.2.5 Issues

Individual (personalised) profiling vs. group profiling

The following remarks are based on a report from FIDIS, an FP6 Network of Excellence on the Future of Identity.[80] Individual and group profiling capacities have grown exponentially as a result of both the huge advances in technology and the increasing availability of readily processable data and traces. Today, an individual – consciously and unconsciously, voluntarily and involuntarily – leaves a vast number of electronic traces in his wake, which can be processed and correlated. The use of the Internet, mobile telephones, electronic financial systems, biometric systems, radio frequency identification tags, smart cards, ubiquitous computing, ambient intelligence and so forth, all participate in the spontaneous and automatic generation of data that can be correlated.

Profiling is a core application which operates by distilling usable information from a large amount of unstructured, raw information. Group profiling technologies build on sameness in the sense of similarity (categorisation); personalised profiling builds on sameness in the sense of unique identification or continuity with oneself. Group profiles are often used to identify persons or to attribute a certain lifestyle, health risks, learning capacity or customer preferences to a person. Even when a group profile does not necessarily apply to the individual members of the group, it may still be used based on the probability that part of the profile does apply. As a result, service providers, insurance companies, forensic agencies, fraud detection departments or agencies and even e-learning organisations use profiling technologies to identify and categorise their target populations. Individual profiles contain personalised knowledge about specific individuals, inferred from off- and online behaviour, registration of birth and/or biometric data.

[80] For a report on FIDISand more information on profiling, see FIDIS, 2005.

The proliferation of automatically generated profiles could have a profound impact on a variety of decisions that influence the life of European citizens. At the same time, it seems unclear whether and how a person could trace back (identify or determine) the sources if and when decisions concerning her life are taken on the basis of such profiles.

Victimisation / Democratic right not be treated as a criminal

AmI technologies could jeopardise the presumption of innocence to the extent that decision-making is delegated to a computer or if a desire for anonymity way is considered suspicious. In the interviews in scenes 1 and 4, we have two examples which illustrate this point: Anonymity profiling and arrest of the clones (one category of user).

Digital divide

The digital divide basically refers to the gap between those communities or groups that have access to Internet, ICTs or any emerging new technologies and those that don't and to the disparities regarding the ability to use them or to learn how to use them. The digital divide is a societal, economic and political issue, all rolled into one. It raises several types of problems and difficulties involving costs, culture, organisation, education, acceptance, adaptation, geography and demographics.

AmI has the potential to bridge certain aspects of the current digital divide but at the same time, it can be assumed that in the future, other and new divides based on AmI technologies will emerge. Problems can be global (between different countries) or local (between different regions in the same country), as raised in scene two. Not every nation or region benefits in the same way or to the same extent from technologies.

AmI may have the potential to exclude and/or include sections of society. Some concerns are raised about the potential of AmI to widen the digital gap between those with access to AmI and therefore to better services and improvements in standards of living in 'smart homes' and those without such access ('digital hermits').[81]

AmI and related technologies could be used as a policy tool and specifically as a tool for innovative social welfare, to improve access to and provision of services for previously excluded or less included groups (e.g., the disabled, ill and elderly).

Dependency

Dependency grows when a technology is widely used. Users become dependent when they do not remain indifferent to the consequences of technology use. This can be joyful when the technology works or frustrating when it does not. The consequences of dependency might affect users in an individual way as well as in an aggregated way. Interview one shows the frustration of a user when his avatar does not fulfil his expectations and in interview three, we see dependency on the system and the subsequent impact when something goes wrong (e.g., traffic jam when a virus affects the system).

[81] FTC, 2005.

Feeling of loss of control

The feeling of loss of control seems to have two main sources: the misunderstanding of the context and the lack of training.

Misunderstandings can arise where there is lack of trust. Misunderstanding of context (prompted by either technical or human factors) can generate dark situations. The table below shows the different cases. Interview four illustrates the case of misunderstanding due to human factors when finally no problem has occurred.

Factors leading to Misunderstanding	**Context**	
	problem	**no problem**
Technical	AmI sensors are not able to detect the problem	AmI sensors detect a problem
Human	AmI sensors are able to detect the problem but the users misunderstand the alert messages	AmI sensors are able to confirm no problem exists but the users don't trust the AmI recommendations

Users often need training to master new devices and services, and this will be also true of AmI technologies because collectively they will create a technological revolution as a function of their ubiquity. Users lacking training lack awareness of the possibilities of the new technologies (services, preferences setting, etc.) and the associated risks. Without a minimum of training, users will likely encounter some in getting services that fulfil their expectations and/or they will be confronted with unwanted AmI behaviour. Consequently, frustration and a feeling of loss of control may arise. Interview one depicts situations of being deprived of access to certain services and being unable to get what one wants as leisure.

Another aspect of loss of control arises when trust is not established between the user and the technology. Trust reassures the user in his willingness to use the technology and in his acceptance of technological behaviour. Trust may be the result from a good knowledge of how the technology works acquired by training or by experience or directly as a result of a positive experience.

Loss of control appears when the interaction between user and a technology is not optimised, transparent or easy (i.e., it is complex). Indeed, this interaction is a crucial point for new emerging technologies. It entails three related challenges:

- user knowledge, i.e., the user should know how to manipulate the technology and to take advantage of the available services,
- "near zero" configuration, i.e., only minimal interaction should be necessary to perform a task,
- trust, i.e., there should be minimal annoyance, minimal limitation on the data needed to use or share a service, adequate protection of user rights, privacy, reputation, etc.

Function creep

"Function creep" is an important concern, i.e., that technology and processes introduced for one purpose will be extended to other purposes which were not discussed or agreed at the time of their implementation.

5.2.6 Legal synopsis

Profiling and unsolicited information

Personal profiling is beneficial to the extent that it enables us to enjoy services and obtain information of interest more easily, but there is a risk that it could be excessive or manipulated. It might be used to refuse certain services, because one has a negative profile. Profiling is based on the collection, processing and transmission of data between different service providers. Clearly, data should be collected and transferred in a lawful way, but current solutions may not be sufficient to provide the proper balance between the risks arising from the profiling, the protection of privacy by limiting data collection, and the workability of a service or system. The obligation of the provider to act in accordance with principle of proportionality may be relevant to resolve the issue. The prohibition of the Data Protection Directive (art. 15) according to which a person may not be subject of a decision solely based on the processing of personal data should be enforced.

Some service providers may abuse new AmI capabilities to engage in unsolicited and unwanted communication for marketing purposes. Currently, the individual can object to such communication, although it puts the burden on the consumer. Individuals may have problems in setting their preferences so that they only receive emergency information and not commercial information, as occurs with the cheap PDA devices that have to be manually adjusted to the mode recommended by the concert organiser. Choosing not to receive commercial communications creates the risk of losing information and services needed by the individual (as in the case of the MEP). The existing rules allow and oblige service providers to make a distinction between practical and commercial information. Still, there are open questions about the enforcement mechanisms of those rules and ability of individuals to react when their devices are abused for commercial purposes.

Liability

Creating the virus, which affected the traffic system, is criminal offence as defined in the Cybercrime Convention (an electronic virus can be regarded as device). The Convention, however, requires proof of the intent to commit the crime. When a virus is created, no specific intention may exist. That is why in some situations the specific intent should not be a precondition of liability. Even when there was no bad intention, the creator might still be liable for the civil damage caused.

Liability of other persons for the damage caused by the virus should also be considered, especially since the creator of the virus will often be untraceable. The different traffic services may neglect to protect their systems sufficiently. Still, it might be too difficult to prove which service provider is responsible for which part of the damage, to prove the fault and the causal link. Similarly, in the case of the person refused by the hotel after insufficient profiling, it would be difficult to establish which provider caused the error, damage and causal link. The evidential issues (procedure) as well as the tort rules and prerequisites (as causation, establishing fault and damage) are regulated by national laws. It will be difficult to meet the traditional tort law preconditions in such situations. On the other hand, the Data Protection Directive states that any person who has suffered

damage is entitled to compensation. Future developments and case law will have to clarify the issue of liability in such cases.

Privacy

Service providers are obliged to ensure safety and security. Safety during the concert may justify certain limitations to the right of privacy of individuals. However, the proper balance has to be created between the need for security and privacy protection. New technology (such as the chips swallowed by people which help the concert organiser to control the safety of the audience which help ensure anonymity) may offer a solution to resolve this conflict. The adequacy of certain new technologies and new solutions offered will have to be assessed in relation to the principles of proportionality and necessity as defined in Human Rights Law.

5.3 CONCLUSIONS

The risk society is the key theme of this scenario. These four scenes depict dark situations, which stem from an inappropriate use, application or management of AmI technologies and which may generate a wide range of impacts on citizens, groups or even society. The four scenes raise private and public concerns, which have local and global scope. The scenes posit several problems related to the proliferation and protection of personal data, user acceptance, dependence, costs and enhancement or loss of trust. The scenario deals with issues including victimisation, digital divide, categorisation of users, dependency, loss of control and function creep.

All of these issues could lead to a major risk, that of an identity crisis. The risks at this level can be seen as a triptych:

- at an individual level, where you are unable to get what you want,
- at a social level, where you may be excluded because of the relatively high cost of new technologies,
- at a societal level, where one may be victimised through loss of social and legal recognition. This means:
  - one may become suspect by default, because acting anonymously may be considered as suspicious
  - one may become an unrecognised person by law and may suffer impersonalisation and/or misrepresentation. Indeed, in cases of fraudulent usage of personal data, it would be difficult to recover a normal situation or reputation in view of the AmI environment's voracious appetite for personal data, a difficulty compounded where the individual lacks adequate legal resources.

6 A DETAILED LEGAL SCREENING OF THE SCENARIOS

This chapter provides a more detailed legal analysis of the scenarios. It is structured according to the four scenarios and the dark situations presented in each. These situations are analysed according to the following structure:

- *Scenario description* presents in brief the facts upon which the analysis is based;
- *Scenario link* contains a quote from the scenario script to indicate the position or significance of the situation in the scenario;
- *Legal field* mentions which legal fields could apply to the situation;
- *Legal chapter* refers to the specific chapter of the legal text;
- *Discussion* is the section where the legal issues and problem areas are developed;
- *Conclusion* contains a short statement on the issue.

6.1 DARK SCENARIO 1: A TYPICAL FAMILY IN DIFFERENT ENVIRONMENTS

6.1.1 Working from home

Situation description	Paul mainly works from home for a private security company. He is a security agent and from his desktop computer at home, he provides remote surveillance of client premises.
Scenario link	*The father (Paul) mainly works from home for a private security company.*
Legal field	Privacy at home and in the workplace.
Legal chapter	Privacy Article 8 ECHR - Data Protection Directive 95/46 - WP 29 Working document on the surveillance of electronic communications in the workplace.
Discussion	Article 8 of the ECHR protects the private home. The problem is that the workplace of the father Paul is situated in his private home and that the workplace is also used, to a lesser extent, for private purposes (including by the members of his family). When Ricardo enters his father's office, he enters a private place and a working place at the same time. The question is whether and how you can make a distinction between both situations, and what the consequences of such ambiguous situations can be from a privacy point of view. In other words: how far does the monitoring of employees go when they work outside the office (at home or in other public or private spaces)? When should monitoring take place if employees work variable hours? What can be monitored and how can a distinction be made between private and professional communications, locations and private life in general?

The European Court of Human Rights has clarified that the protection of private life does not exclude the professional life as a worker, and that protection isn't limited to life within home. In *Niemitz v. Germany* (23 November 1992), the Court stated that there is no reason why the notion of "private life" should be taken to exclude activities of a professional or business nature. Moreover, the Court added that this view is supported by the fact that "it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not." In *Halford v. United Kingdom* (27 May 1997), the Court introduced the criterion of the "reasonable expectations of privacy". Accordingly, Miss Halford, a senior officer whose telephone calls were intercepted without warning, was granted privacy protection in her office space, although not absolute. More case law is needed in the future to clarify the implications of the criterion of "reasonable expectations of privacy". Its introduction by the Court seems to suggest a new future for privacy conceptualisation. However, the use of it by the American courts has shown a development towards an erosion of legal privacy protection. Americans have fewer expectations that their privacy will be protected by the courts.[82]

Protection of privacy at the workplace remains one of the grey areas in European human rights law. The case of Halford, a senior officer with privileges, is in itself not a typical case. More case law is needed to clarify the European use of the criterion of reasonable expectation of privacy in the context of more straightforward examples regarding the workplace. It should also be borne in mind, that surveillance of the individual after a suspicion has been raised, raises less concerns than the general surveillance at a workplace, public building or home. The latter however may still become more the case in AmI and in the situation dealt with in the scenario. It is unclear how and if the reasonable expectation of privacy would apply in such situations. While being always on-line, would we be able to talk of any expectation at all?

An additional problem is the lack of clarity regarding the consequences of privacy violations. The European Court is willing to extend privacy protection outside the traditional realms and to include aspects of workplaces and public places, but is unwilling to recognise a right to have evidence obtained through privacy violations rejected in the court. In cases such as *Khan* (2000) and *P.H. & P.G. against the United Kingdom* (2001) the Strasbourg Court on Human Rights decided that a violation of Article 8 ECHR had taken place, but it nevertheless accepted the use of the evidence found in violation of Article 8 ECHR in a criminal process. This line of reasoning is followed by at least some national courts. In Belgium, there are examples of the erosion of privacy law in the

[82] See for examples: GOLDMAN, J., 'Privacy and individual empowerment in the interactive age' in POULLET Y., DE TERWANGNE C. & TURNER P., *Privacy: new risk and opportunities*, Diegem, Story-Scientia, 1997, 70-71

workplace: The Belgian Data Protection Act (1992, revised in 1998) and Collective Labour Agreement 68 of 16 June 1998 foresee that strict procedures of information and negotiation must be followed when cameras are installed in the workplace. Thus, employees must be informed when an employer installs cameras. The "Cour de Cassation", the highest Belgian court, argued in a recent case that Articles 6 and 8 ECHR don't necessarily mean that the infringement of the information and negotiation procedure laid down in data protection law void the evidence obtained with a hidden camera (in this case, a theft by an employee)[83].

Conclusion Article 8 of the European Convention of Human Rights protects the private and family life, the home and communication. The Court of Strasbourg has stated that this does not *a fortiori* exclude professional activities. Moreover, the protection offered by Article 8 is not limited to specified spaces and/or places. AmI will probably impose a redefinition of the terms home and communication, as well as a reinterpretation of the term private life, since the distinction between private life and professional life might become further blurred. It is unclear how and if the American criterion of "reasonable expectations of privacy" will further be applied by the European courts. It is equally unclear how this criterion will apply in an AmI world. If the privacy case law does not offer sufficient and clear privacy protection of AmI environments, additional legal and constitutional protection may be warranted.

6.1.2 Digital rights management

Situation description Ricardo invites his friends to play an online game at his place because only Ricardo has a licence for it. This online game licence can be linked to an IP number or with DRM applications.

Scenario link *"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."*

Legal field Privacy, data protection and intellectual property

Legal chapter Data Protection Directive 95/46 - Copyright Directive 2001/29 - Directive 93/13 on unfair terms in consumer contracts - Directive 97/7 on consumer protection in respect of distance contracts - E-Commerce Directive 2000/31 – Freedom of Expression

Discussion New intellectual property business models are emerging in the sector of copyrights, gaming and other forms of on-line

[83] See more in general: Nouwt, S., de Vries, B, & Prins, C. ,2005. See also the Judgment of the Belgian *Cour de* Cassation of 2 March 2005: http://www.juridat.be.

entertainment. Where people used to buy physical carriers that incorporated a work of art (a book, a DVD), this has fundamentally changed. In our AmI future, instead of owning the physical carrier (corpus mechanicum), people will buy a licence to *access* the work online. According to the licence, they can use the copyrighted work only once, twice, several times or just download it from a certain physical place (an IP address, as in this scenario) or from a certain device (such as a PDA or mobile phone). In order to manage the access rights through the DRM systems, the owners of copyrights will monitor how many times users access the work, how long they consume the content, what other content they like, etc. Only upon an identification and authentication of rights to the content will the user be able to access the content. DRM systems allow content holders not only to process personal data (user behaviour), but also to construct (group) profiles, building statistics, viewing consumer behaviour, etc. Here again, personal data are stored for a longer period and for purposes of which the user may not always be aware.

Such developments conflict with some of the main principles of data protection law, namely, the purpose specification principle and the principle of proportionality expressed in Article 6 of Data Protection Directive 95/46. According to this Article: "*1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use; 2. It shall be for the controller to ensure that paragraph 1 is complied with.*"

Especially the proportionality criterion laid down in sub (c) obliges policy-makers to consider alternative, less infringing ways of reconciling intellectual property rights with privacy rights.

Such developments might also prevent users from anonymously "consuming" (reading, viewing, listening to) "information". This evolution is supported by article 6 of the Copyright Directive, stating that "*Member States shall provide adequate legal protection against the circumvention of any effective technological measures,*

which the concerned person carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective." Consequently, technological measures such as DRM-systems might function at the same time both as a tool for digital rights management *and* as a tool for profiling and modelling users who (anonymously or not) are monitored in order to support the functioning of the DRM system. This can also lead to price discrimination when personalised advertising and pricing occurs.

The argument of freedom of expression will probably prove to be one of the more powerful in the future against rights management systems that are based on individual identification. Monitoring persons that consult work, such as books, will make people refrain from reading certain books and will create an environment that is destructive of freedom of speech and thought.

Conclusion General principles of data protection and freedom of expression and thought oppose digital rights management systems and applications that rely on unnecessary individual monitoring or are used for purposes other than DRM, such as profiling, especially when these other uses are often imposed in a non-negotiable way. Possible solutions may be found in e-commerce and consumer protection law, by giving, for example, more legal (and technological) possibilities to consumers to negotiate use of their personal data.

6.1.3 ID theft and liability

Situation description Ricardo can access – through the duplication of an iris scan and the circumvention of the security measures – his father's office, computer, profile and preferences.

Scenario link *"Ricardo is indeed enjoying himself with his friends in Paul's study. They were able to enter because the door was still open. At last, he has the opportunity to check whether the print-out he has of his father's iris can fool the iris scanner which it must do, if Ricardo is to unlock his father's computer. It does!*"

Legal field Security and confidentiality obligations imposed on data controllers and data processors.
Hardware and software security in general.
Liability for defective software and hardware.

Legal chapter Data Protection Directive 95/46 - Directive 85/374 on liability for defective products.

Discussion Who is responsible for the fact that Ricardo could enter the office and obtain his father's profile? Was the system developed in a way sufficient to prevent manipulation one of the kind described in the

scenario? Was the father careful enough to shut it down and did he put the confidential information in his office in jeopardy?

Compliance with the security obligations, amongst others those expressed in Article 16 and 17 of the Data Protection Directive 95/46, is not clearly regulated. When Paul works at home or at any place in the AmI environment and processes personal data of data subjects, for example, his employer's clients, strict compliance with Data Protection Directive law is needed. This means that the "*controller must implement appropriate technical and organizational measures to protect personal data, in particular where the processing involves the transmission of data over a network, having regard to the state of the art and the cost of their implementation. Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. The controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating amongst others that the security obligations shall also be incumbent on the processor*" (Article 17 of Directive 95/46).
It is not clear, however, how far the obligations of both the data controller and the data processor (acting under the responsibility of the data controller) go. Who is responsible for the security of the home network that is used for tele-work? Is the employer obliged to secure at his risk and at his cost the home-work environment of the employee? Who – the employee or the employer – is responsible if personal data relating to customers are copied, altered or stolen through the employee's home network as a consequence of a lack of security? How can the security of the home system network be controlled by a third party? When is the employer liable when something goes wrong with personal data, and when the employee?

Ricardo was able to enter his father's office relatively easily and to appropriate his profile. The office contains important information about the company and Paul should have ensured that his son could not access it. When the father joined the company, the labour contract probably contained clauses that allowed him to work at home under the strict condition that he protect and respect the confidentiality of the information he obtains during his activities. If some of the confidential information became known to unauthorised people, the father might become liable towards the company and might be fired.

Another possibility is that Ricardo was able to enter the system, to hack the profile and to view the confidential information (both

private and professional information) due to defects of the security system (hardware or software). The question is whether the provider of the security software can be held liable and to what extent this liability can be waived in general terms and conditions. Today, software products licence agreements clearly indicate that the software is purchased without liability for the loss of information. In this scenario, it is not clear if the defects, if any, are situated in the software or hardware. On the basis of actual regulation, this is important: Article 1 of Directive 85/374 on liability for defective products provides that the producer of a product is liable for damage caused by a defect in his product. A product, however, is only defective when it does not provide the "*safety which a person is entitled to expect*", taking all circumstances into account, including (a) the presentation of the product; (b) the use to which it could reasonably be expected that the product would be put; (c) the time when the product was put into circulation. A product shall not be considered defective for the sole reason that a better product is subsequently put into circulation. A product, however, is defined as "*all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable.*" It is unclear today whether this directive applies to defective software and/or hardware. Also, it is not clear if and to what extent economic damages fall under the concept of damage (injury) in the sense of the directive.

If this directive applies to the scenario (if there is a defect in the security hardware or software) this means the following: normally the victim has to prove that the producer committed a fault, which is much more difficult to prove then demonstrating that the product is defective. Since the security system was insufficient to prevent the son from using his father's profile, we could consider the system to be defective. An important question is, of course, which producer caused the defect and how to find him. Article 3 of the directive states clearly that when the producer of a product cannot be identified (which might be a serious problem in an AmI world), "*each supplier of the product shall be treated as its producer unless he informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product*". On the basis of Article 5, two or more persons shall be liable jointly and severally when they are liable for the same damage. This implies that if several service providers are co-responsible for the defect, the victim can claim the total damages from one of them, probably his direct supplier. In certain specific situations, defined in Article 7, the producer can limit his liability. Article 8 sets out an important principle: "*The liability of the producer shall not be reduced when the damage is caused both by a defect in the product and by the act or omission of a third party*". But there is an important nuance: "*The liability of the producer may be reduced or disallowed when, having regard to all the circumstances, the damage is caused both by a defect in the product*

and by the fault of the injured person or any person for whom the injured person is responsible." A producer does not have the possibility under this directive to invoke the fault of others to escape his liability when his product was defective. He can reduce his liability when the victim was co-responsible, as in this case where the father has been negligent. Finally Article 12 states that "*the liability of the producer arising from this Directive may not, in relation to the injured person, be limited or excluded by a provision limiting his liability or exempting him from liability*."

Conclusion

All controllers and processors, especially in professional circumstances, must be aware of the security and confidentiality requirements applicable to the processing of personal data as formulated in Articles 16 and 17 of the Data Protection Directive 95/46 and Articles 4 and 5 of the Privacy and Electronic Communications Directive 2002/58. National legislations should be harmonised to organise data protection and security measures in tele-working conditions and clear policies should be agreed upon.

The issue of strengthening the security and confidentiality provisions in the directive with criminal law sanctions should be considered. The current directives do not foresee this with the practical result that in many Member States there is no criminal sanction for violation of the duty to foresee sufficient safeguards. Especially when unique identifiers are used for processing purposes such as security, lack of protection should be considered a serious act. A second option is to foresee in specific measures with regard to the use of biometric data and to prohibit badly protected or too risky use of biometrics.[84]

The Directive 1985/347 on liability for defective goods does not apply to services and presumably not to computer software. The solution proposed in the Directive should be broadened and adapted to services and computer programs related to AmI.

6.1.4 Inadequate profiling

Situation description

The inadequate profiling can lead to innocent people being investigated or impeded in one way or another.

Scenario link

"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… He is disappointed to miss a promotion now, but he is confident that the opportunity will come around again."

[84] See De Hert, P., 2005.

Legal field Profiling & Security – Privacy and Data Protection – First & Third pillar of the EU

Legal chapter Data Protection Directive 95/46 – Privacy & Electronic Communications Directive 2002/58

Discussion When personal data about an individual are collected and processed, the personal data as well as the information derived from the personal data should be correct.

The Data Protection Directive 95/46 states in Article 6 (a) that the data must be processed fairly and lawfully and provides a protection for the individual against incorrect data. Article 6 (c) and (d) provide that personal data must be adequate, relevant, accurate and kept up to date. It further stipulates that "*every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.*"

In this scenario, the data subject does not understand why the cyber police suspect him of a certain crime. In order to be able to defend himself against these accusations, he will need to know which personal data the cyber police collected and processed. Again, Data Protection Directive 95/46 foresees this possibility. Article 12 (a) provides that every subject has the right to obtain from the controller "*without constraint at reasonable intervals and without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; communication to him in an intelligible form of the data undergoing processing and of any available information as to their source; knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions.*"

This information should allow him to know why he is suspected and might allow him to prove that he is not the person the cyber police are searching for. On the basis of Article 12 (b) of Directive 95/46, the data subject has to obtain from the controller "*as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.*" This would allow him to correct his profile as created by the cyber police. Also, the data subject can ask on the basis of Article 12 (c) of Directive 95/46 that any rectification, erasure or blocking carried out be notified to third parties to whom the data have been disclosed, such as Paul's employer.

The cyber police treat him as a suspect, because 35 per cent of his profile fits with that of a perpetrator of a crime. The decision to ask for extra information from his employer on the basis of this 35 per cent match is a decision based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his reliability and conduct. Article 15 of Directive 95/46 provides that every person has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is solely based on such an automated processing of personal data. A person may be subjected to such a decision if that decision is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests. This clearly implies that such a decision can only happen in exceptional cases. The decision of the cyber police to ask extra information to the employer might have important consequences. Consequently, this legal tool should be used carefully.

The foregoing is based on principled reasoning.

First, current choices for new policing and anti-terrorism strategies seemingly pave the way for the acceptance of police practices based on profiling. The principle of availability, for example, included in the The Hague Program of the EU is instrumental for a policy of greater data protection flexibility for the police.

Second, it is well-known that Directive 95/46 is a first pillar Directive that does not apply to activities in areas of criminal law and in any case not to processing operations concerning public security, defence, State security (Article 3.2.). These services are governed by national data protection laws that are not harmonised by an instrument of the EU.

Third, it is clear that the more and longer electronic communication data (traffic data) are retained, the greater are the possibilities for the police to collect and process the personal data and to build and use profiling techniques upon these data for their work. According to first pillar Directive 2002/58, electronic communication data must be deleted when they are no longer needed for the provision of the service or for the billing thereof. However, Directive 2002/58 does not apply to activities in areas of criminal law and in any case not to processing operations concerning public security, defence or State security (Article 1.3.).

The fact that both Directives 95/46 and 2002/58 don't apply to those activities should be related to two regulatory initiatives at EU level with regard to the retention of electronic communication data by Internet service providers for a period longer than the terms foreseen in Directive 2002/58. On the one hand, there is a draft framework decision for the retention of electronic communication data for a minimum period of one year (third pillar), submitted in April 2004

by France, Ireland, Sweden and the UK, and the proposal for the Council Framework Decision on the protection of the personal data processed in the framework of police and judicial cooperation in criminal matters (COM (2005) 475 final).. On the other hand, there is a proposal for a directive, adopted in September 2005, to retain data related to the usage of mobile and fixed telephony as well as the Internet communications for a period of one year and six months respectively (first pillar). This proposed directive would also amend Directive 2002/58.

The national police data protection bills have to be in line with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108. With regard to police and other third pillar issues, however, the provisions of the 1981 Convention are very sober. The 1981 Convention contains no provision comparable to Article 15 of Directive 95/46/EC. This is only partly compensated for in Recommendation No. R(87)15 regulating the use of personal data in the police sector (17 September 1987). The Recommendation, a soft law instrument developed by experts in the context of the 1981 Council of Europe Convention, is not legally binding and was conceived in an era that was unaware of (or unwilling to accept) new forms of systematic and intelligence-led policing. If our police forces were to apply the Recommendation today, they would have no choice except to collect data only when there are sufficient grounds to do so and to destroy such data as soon as possible. Clearly, this is not in line with current choices for new policing and anti-terrorism strategies.

Conclusion EU Directives 95/46 and 2002/58 do not apply to the use of profiling techniques by the police. The EU is currently considering the idea of drafting a third pillar data protection instrument. The merits of this initiative need not be underlined. There is a strong need for a coherent instrument for the protection of personal data under the fields now covered by Titles V and VI of the EU Treaty. Current police strategies such as profiling should be considered within the scope of such new instruments. A framework that is favourable to profiling practices as described in the scenario is not unthinkable, although it represents undeniably a rupture with the current legal framework in criminal law.

6.1.5 Monitoring behaviour

Situation description Ricardo shuts off the parental control system that can monitor his behaviour.

Scenario link *"With his father's profile and identity, Ricardo can circumvent the parental control system that governs use of the Internet by all terminals in the home."*

Legal field	(Online) Privacy for children
Legal chapter	Privacy Article 8 ECHR – 1990 United Nation Convention on the Rights of the Child
Discussion	Paul and Maruja installed a system to monitor the digital movements of their children. It does not function, since the son disabled the system, but should the parents be entitled to do that in an AmI world (even outside the private home)? Has Ricardo the right to protect his privacy, since he is in his own home? Article 8 of the ECHR protects the private life of every natural person and thus that of Ricardo. Although Paul may have certain rights to control what his children are doing, this should, in principle not be exaggerated for these rights are to be balanced. The United Nations Convention on the Rights of the Child (1990) contains a specific privacy right for children. Without denying parental rights, this UN Convention adds more weight to the privacy rights of children. The Convention also sets up monitoring instruments such as National Children Rights Commissioners. "New" problems such as the digital monitoring of children will thus also have to be taken up by National Children Rights Commissioners. It is unclear what the outcome of this balancing act will be. Permanent monitoring infringes on children's privacy rights, but it might be looked upon as a way of or price for granting more physical liberty to children.
Conclusion	"New" problems such as the digital monitoring of children will also have to be taken up by National Children Rights Commissioners.

6.1.6 ID theft and payments

Situation description	Ricardo uses his father's profile to make payments, whereas the father did not agree to the payments and the minor is probably not capable of concluding contracts independently.
Scenario link	*"Ricardo places a bet on a sports gambling site, downloads some xxx-rated movies and games on his personal space on the family server and checks out his father's online favourites… Ricardo laughs. But he won't be laughing when his father finds out that Ricardo has spent 200 euros from his account. "*
Legal field	E-commerce and Consumer Protection Law. Electronic Identification.
Legal chapter	Directive 97/7 on consumer protection in respect of distance contracts - E-Commerce Directive 2000/31.
Discussion	When the son bought goods or services on the Internet, the contract

he concluded had to respect certain terms and conditions. In this situation, several of the basic conditions are not fulfilled. The first important question is whether we can talk about consent. Although it seems like the father via his profile provides consent to the agreement, he was not even aware of it. If the son was too young, the son does not have the capacity to conclude the contract. Ricardo misleads the system, but we can ask how much effort the service supplier should make to ensure that he verifies who the real customer is (authenticating the credit card would not be enough).

Article 4 of Directive 97/7 obliges the supplier to provide to the consumer in good time prior to the conclusion of any distance contract, specific information related to the contract. This obligation was created to protect the consumer and it refers specifically to the principle governing the protection of those who are unable to give their consent, such as minors. There might be discussion about the fact whether Ricardo, as a minor, was able to conclude the contract. The service providers will probably tackle this by putting in the terms and conditions a requirement that the customers have to protect their identity and that they are responsible for any abuse of it. Article 6 provides for a right of withdrawal: "*For any distance contract the consumer shall have a period of at least seven working days in which to withdraw from the contract without penalty and without giving any reason. Where the right of withdrawal has been exercised by the consumer pursuant to this Article, the supplier shall be obliged to reimburse the sums paid by the consumer free of charge.*" In principle, the father could use this right of withdrawal to cancel the contract.

He will not be able to exercise this right, however, in respect of contracts "*for the provision of services if performance has begun (such as downloading X-rated movies), with the consumer's agreement, before the end of the seven working day period, and also for the supply of goods made to the consumer's specifications or clearly personalized or which, by reason of their nature, cannot be returned or are liable to deteriorate or expire rapidly; for the supply of audio or video recordings or computer software which were unsealed by the consumer, for gaming and lottery services (such as on-line betting).*" It is likely that the goods or services bought by Ricardo fall under one of these exceptions.

Also, even if the father were able to exercise his right of withdrawal, this is sometimes difficult to achieve when the money has been taken from one's account. Sometimes, goods and services are delivered by companies that are not transparent or physically situated outside the EU and they are not willing to pay the money back.

The directive on the protection of consumers in respect of distance contracts will thus not offer much assistance. What could help is the

creation of a trusted third party that receives the payments on behalf of the service provider, while keeping the amount of the payment automatically in a temporary account, until the right of withdrawal has expired.

Also Directive 2000/31 protects consumers in the domain of e-commerce. It sets out a number of important information obligations on the service provider. It does not offer, however, a complete solution to this concrete problem.

Conclusion Automated payments make it easy to spend money quickly. Distance contracts do not offer the same guarantees, trust and confidence as in physical commerce. Protection of consumers against unwanted e-commerce actions and distance contracts can be supported by trusted third parties who act as intermediaries.

6.1.7 Spyware and personal preferences

Situation description A spyware program collects personal data and preferences, *inter alia*, to target data subjects with personalised advertising.

Scenario link *"Neither Maruja nor Elena are aware that the website with the attractive offer contains a powerful spyware program that looks for personal data and preferences, so that users can be targeted with personalised advertising. The spyware helps to reveal a person's attitude towards privacy and spam."*

Legal field Privacy and security - illegal data collection - spyware.

Legal chapter Data Protection Directive 95/46 - Cybercrime Convention of 23 November 2001

Discussion The use of spyware clearly constitutes an infringement of the basic principles of data protection law (Directive 95/46). Article 6 of the Data Protection Directive provides that personal data must be processed "fairly and lawfully", a provision which is linked to the transparency principle and the desired openness of processing. In principle, the data subjects have to be truly and fully informed about all phases and contexts of the processing procedure. Of course, this is a *condition-sine-qua-non* for subsequent controls on data processing. It specifically applies to the gathering of personal data, which should not be based on secret, hidden or sly methods. The secret, hidden gathering and processing of personal data or the hidden use of microphones, cameras, listening devices, detectors and programs are in principle prohibited. No openness, no legitimacy. Moreover, according to the purpose specification principle (supra), personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. To be legitimate, according to Article 7 of the Data

Protection Directive, personal data may only be processed if the data subject has unambiguously given his consent or if the processing is necessary in certain situations which are clearly not covered in the case of spyware.

In general, seen from the perspective of the conditions set forth in the Data Protection Directive, spamming presupposes illegitimate data collection, sharing and selling (data laundering, see next situation). That is why the stringent opt-in rule of the Privacy and Electronic Communications Directive imposed itself. Moreover, if a customer has opted for direct marketing, he mostly remains unable to know upon which personal data and information direct marketing actions are based.

The use of spyware programs (installing and spying) constitutes a number of criminal offences according to the Cybercrime Convention: illegal access (Article 2) and illegal interception (Article 3) when there is, in the latter case, an interception, without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system. Not only is the use of spyware a criminal offence, but also (Article 6) the production, sale, procurement for use, import, distribution or otherwise making available of (1) a device, including a computer program, designed or adapted primarily for the purpose of committing (in this scenario) illegal access and interception, (2) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing (in this scenario) illegal access and interception. Even the possession of such items can constitute a criminal offence.

Conclusion The problem of spyware can be addressed with the technical solutions; however from the legal point of view it seems to be one of these problems that obviously cannot be solved within data protection only. Despite the fact that deterrence by criminal law is always the last recourse, there is a case for inserting criminal law prohibitions on the use of spyware in national criminal codes.

6.1.8 Data laundering

Situation description Data laundering. Via a large number of transactions and operations, the illegal origin (illegal collection) of personal data can be camouflaged.

Scenario link *"Companies are paying a lot of money for personal and group profiles.*[85] *This phenomenon is known as "data laundering". Similar*

[85] Vijayan, Jaikumar, "ID Theft Continues to Increase. More than 13 million Americans have been victimized, new study reveals", *Computerworld*, 30 July 2003.
http://www.pcworld.com/news/article/0,aid,111832,00.asp

to money laundering, data laundering aims to make illegally obtained personal data look as if they were obtained legally, so that they can be used to target customers."

Legal field Privacy and data protection – Data Laundering.

Legal chapter Data Protection Directive 95/46 - Cybercrime Convention of 23 November 2001.

Discussion By definition, data laundering is a violation of data protection legislation, since it hides the fact that personal data were illegitimately processed.

We might need to foresee specifically that persons and companies that are involved or assist in the laundering of data be subject to penal sanctions.

Especially companies can participate in data laundering. A way to prevent data laundering could be the 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. Without checking the origin and/or the legality of the databases and profiles, one could consider the buyer equal to a receiver of stolen goods.

Another possibility is to apply the rules of money laundering in a similar way to data laundering, for example, by the obligation to notify the national data protection officer when, how and from whom personal data are acquired.

Conclusion Data laundering via large uncontrolled (commercial) traffic of individual profiles and personal data could become one of the "escape routes" in the struggle against data protection infringements. There are no clear provisions for this in criminal law, but there could be so that a crime is committed when databases of obvious illegally collected personal data are acquired.

6.1.9 Location-based advertising and spam

Situation description Location-based advertisements and location-based spam increases due to new communication devices.

Scenario link *"She is receiving almost continuously messages on the flexible screen on her sleeve.[86] She likes the blouse she borrowed from her friend to test the on-screen possibilities of this smart piece of clothing. The screen shows there is a tai-chi gathering on the east*

Zetter, Kim, "TSA Data Dump Leads to Lawsuit", *Wired News*, 14 July 2005. http://www.wired.com/news/privacy/0,1848,68560,00.html

[86] Espiner, T., "Philips unfurls prototype flexible display". http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39216111,00.htm

side of the park. She might want to join because of her interest in relaxation exercises and in Eastern philosophies." (…)

"Another ad appears: 'Special offers from the bookshop next door.' Maruja gets annoyed by the location-based spam and decides to switch off almost completely, only allowing incoming 'emergency' messages."

Legal field Unsolicited communication - Spam - Location based advertising – E-commerce and Consumer Protection.

Legal chapter Data Protection Directive 95/46 – Privacy & Electronic Communications Directive 2002/58 – E-commerce Directive 2000/31.

Discussion Individuals are influenced by the information they receive. In order that an individual can control his own reality to a certain extent, the person must somehow control whether or not he wants to receive electronic information and communication.

Unsolicited electronic communication for the purposes of direct marketing is prohibited, although exceptions exist, for example, in an existing customer relationship. In principle, however, the Privacy & Electronic Communications Directive 2002/58 installs an opt-in system, implying the prior consent or wish of the subscriber. Other obligations are that the identity of the sender may not be disguised or concealed and that each message must contain an electronic address so that the receiver can easily opt out.

One can argue that the "unsolicited communications" chapter of Privacy and Electronic Communications Directive 2002/58 may not apply in some situations. First of all, the article is about commercial communications (see recital 40), so that non-commercial communications fall outside the scope of Article 13. This may not be such a problem since almost all information is of a commercial nature.

But, in addition, in order to apply the opt-in rule, it must be a commercial "communication". A "communication" is defined in the Directive 2002/58 as "*any information exchanged or conveyed between a finite number of parties by means of publicly available electronic communications service. This does not include*," continues the definition, "*any information conveyed as part of broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.*"

One can argue that the opt-in obligation does not apply when the messages are sent to (sleeves or other devices that belong to)

anonymous persons. In that case, the information cannot be related to an identifiable subscriber or user receiving the information. One can also argue that, if messages are "broadcast" to everybody who enters a certain area or walks in a certain park or street with his device on, this case can fall outside the scope of the directive as well: There is a constant broadcast in Elm Street and every person walking in Elm Street with his device on can be compared to a person switching his TV from channel X to channel Y.

United States case law has confirmed that pop-ups (small windows separately popping up when visiting a website, often containing commercial information) do not infringe anti-spam law (Utah Court of Appeals, Jesse Riddle vs. Celebrity Cruises, 30 December 2004, available with comments through http://www.droit-technologie.org/1_2.asp?actu_id=1038).

The e-commerce Directive 2000/31/EC also contains important provisions on commercial communications. Irrespective of the question whether commercial communications are wanted, Article 6 states that "*commercial communication which are part of, or constitute, an information society service should comply at least with the following conditions: (a) the commercial communication shall be clearly identifiable as such; (b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable; (c) promotional offers, such as discounts, premiums and gifts shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;(d) promotional competitions or games shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously." "Unsolicited commercial communications shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient. Service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.*"

Although they exist on a worldwide scale, spam laws do not stop spam. Spam is sent by billions everyday, and spam filters and other machines do the work. If people in the EU are confronted with spam, they have great difficulties to undertake civil actions because they can not find the sender of the spam and if they do, they can not prove the damage (which is indeed low, from an individual point of view) in a procedure which is too expensive. In the US, fixed civil remedies are often foreseen by state laws (among others in Arizona, Arkansas, Connecticut, Illinois, Minnesota, New Mexico, North Carolina), for example, 10 USD per spam received.

Conclusion Spam not only takes time and provokes irritation, but also can

influence and infringe someone's private world. Both Directives 2002/58 and 2000/31 contain provisions on (unsolicited) commercial communication, but do not really seem to have the desired effect. Legal certainty should exist towards the enforcement of spam law and towards new methods and applications that are used to approach people with (commercial) communications in an AmI world.

6.1.10 RFID-tagged blouse

Situation description

Burglars have read the blouse that Maruja wears. This blouse contains an RFID chip. The RFID chip contains information about the shop where it was bought and the thieves hack the shop's database to find out where the buyer of the blouse lives. Because the blouse was borrowed from a friend, the burglars confront this friend when they break into the house.

Scenario link

"The burglary and mugging occurred because of an unlucky coincidence of circumstances, i.e., that Maruja was wearing Claire's blouse when she went to the park where the criminal gang happened to be operating. As she was passing by, the gang "read" the RFID tag embedded in the blouse. As a result, the gang found out that the blouse had been sold at a certain shop. The gang hacked the client database to discover Claire's profile (a well-off woman living alone in the richer part of the city).[87] On the assumption that Claire was wearing the blouse, the criminals decided to break into the apartment and to steal whatever luxury goods they could find."

Legal field

Privacy and data protection – criminal law – computer hacking and abuse of personal data for criminal purposes – liability

Legal chapter

Privacy Article 8 ECHR – Data Protection Directive 95/46 – Cybercrime Convention of 23 November 2001 – Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

Liability – Directive 85/347 concerning liability for defective products (Cf. section 6.1.3)

Discussion

The blouse might be considered as a part of one's private life in the sense of Article 8 ECHR and should, in principle, not be accessed by unauthorised people. The personal data contained and processed in the RFID-blouse are definitely a matter falling under the rules and conditions of data protection law which does not allow secret and unfair collection of personal data. Not only the personal data contained in the blouse, but also the blouse itself falls under data protection law since it can be related to an identifiable person: The

[87] Knospe, H., Pohl, H., 2004.

RFID tag that identifies the object is connected with the purchase data that identify the subject.

Moreover, when the burglars accessed the information in the blouse they committed offences defined by the Cybercrime Convention, such as illegal access, possibly illegal interception. Illegal access is defined by the Cybercrime Convention as, "*when committed intentionally, the access to the whole or any part of a computer system without right.*" Illegal interception is, "*when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data*".

The Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems defines illegal access, data and system interference. Article 3 (illegal system interference) obliges the Member States to "*take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.*"

We also refer here to section 6.1.3 above, where liability for defective software and hardware is discussed. One can argue that the RFID chip (hardware) and the embedded protection software were defective products, causing damage to Maruja, because they were easy to access while the user does not have any control over it. According to Directive 85/347, a product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including the presentation of the product, the use to which it could reasonably be expected to be put and the time when the product was put into circulation. A product shall not be considered defective for the sole reason that a better product is subsequently put into circulation.

Conclusion

It is important to have a common definition of these criminal activities, since they often have a cross-border dimension. The Convention has been ratified by a limited number of countries so far and gives participating countries the option to set extra conditions for described actions to be a criminal offence. This freedom limits the harmonisation.

The Council Framework Decision 2005/222/JHA obliges the Member States of the European Union to take the necessary measures to comply with the provisions of this Framework Decision by 16 March 2007. The Member States of the European Union are thus more bound by this instrument than by the Cybercrime

Convention. The Framework decision is limited, however, both in scope and territory, since it only defines a limited number of crimes and is only applicable to the 25 Member States of the European Union.

It is also important to review the liability for defective (insecure) networks, software and hardware.

6.2 SCENARIO 2: SENIORS ON A JOURNEY

6.2.1 Bus accident caused by hacker

Situation description

Bus accident caused by hacking and abusing traffic lights management system by a minor. Which (criminal) law is applicable, which court is competent and is the hacker the only person responsible?

Scenario link

"*The accident we were involved in was, as we learned later on, caused by a kid who illegally used software for priority vehicles like ambulances and police cars.*"

Legal field

Criminal law – Liability – International Private Law.

Legal chapter

Cybercrime Convention of 23 November 2001 – Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems – Liability – Directive 85/347 concerning liability for defective products.

Convention of Rome on the Law Applicable to Contractual Obligations – Regulation 44/2001 on jurisdiction and enforcement.

Discussion

We can have a cross-border legal conflict: the hacker can be situated in country A; the hacking software can be manufactured and sold by another person in country B; the traffic lights controller (who might not have secured the traffic light system well enough, taking into account the state of the art) is situated in country C; the network provider, through which the attack was easily performed, is situated in country D. The accident takes place in Florence, a city in country E. Which law is applicable and which courts are competent? Who is liable and to what extent, since many actors are involved: the hacker, the hacker's companion, the manufacturer and distributor of the hacking tools, the traffic lights manufacturer and controller, the network providers through which the hacking took place, the bus driver…

Other rules of jurisdiction apply in (civil) liability matters and in criminal law.

Criminal law aspects

In the current framework, there is no binding European regulatory framework that determines jurisdiction in criminal matters. Member States are free to choose their own rules. The basic rule is the rule of territory: states can incriminate actions that happen on their territory. The notion of territory is, however, open to interpretation. Many Member States broaden their jurisdiction by using "expansive" criteria such as the criterion of ubiquity. The result is that for transborder crime, several Member States find themselves competent at the same time for the same facts. This process is not a process of legislation, but of case law.

One can say that there is a tendency in the case law of national judges to interpret the principle or ground of territorial jurisdiction extensively. Belgium judges are not, except for explicit statutory provisions, competent in extraterritorial cases. Legal practice shows that judges give great leeway for Belgian legal authorities when crimes are committed outside Belgium territory but impinge on Belgium interests. The legal situation in Belgium and the Netherlands, and a country such as Chile that also belongs to the civil-law tradition is very similar. In all these countries there are several accepted theories, criteria or answers to the *locus commissi delicti* question, viz. the question to what extent a wrongful act can be considered to fall within the territorial jurisdiction of a state. Within the Dutch and Belgian tradition, the following accepted criteria are applied:

- the activity criterion – the territory where the activity took place is the relevant one;
- the criterion of the instrument of the crime;
- the criterion of the constitutive consequence; and
- the ubiquity criterion – the *locus delicti* is every country where one of the constitutive elements of the crime can be located; it is therefore very well possible that an offence falls within the jurisdiction of more than one country.

Unlike in Germany and France, neither the Dutch nor the Belgian Criminal Code contains a real choice for one of these criteria; it is left to the courts to determine. An analysis shows that whatever criterion is applied, it is almost always easily possible for a judge to declare himself competent and to hold that the events took place on "his" or "her" territory. The ubiquity criterion in particular, by now the most successful criterion within the civil-law tradition, enables a flexible approach towards the *locus commissi delicti question*. It allows countries to prosecute persons spreading computer viruses or racist information from computers abroad, or persons who "call" in by telephone from abroad when this conversation forms the starting point for a crime. The flexibility of the ubiquity criterion explains without any doubt the total absence of jurisdiction provisions in the Belgian and Dutch Computer Crime Acts.

To avoid conflicts of jurisdiction, an international solution is preferable. Currently, there is no such thing as a stringent set of rules with regard to determining territory.
A small paragraph in the Cybercrime Convention tries to remedy this conflict by imposing a guideline that "*the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.*"[88] A bit firmer is Article 10 paragraph 4 of the 2005 EU Framework Decision on attacks against information systems: "*Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralizing proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the coordination of their action. Sequential account may be taken of the following factors:*
- the Member State shall be that in the territory of which the offences have been committed according to paragraph 1(a) and paragraph 2,
- the Member State shall be that of which the perpetrator is a national,
- the Member State shall be that in which the perpetrator has been found." Although these guidelines are not legally binding, there is some wisdom in them. Future experiences will indicate whether more stringent rules are needed.

It is also important to focus on the different possible defendants.

The hacker can be difficult to track. He commits a number of criminal offences defined in the Cybercrime Convention, such as "illegal access", "illegal interception", "data and system interference" and possibly "computer-related fraud".

The producer, seller or distributor of hacking software might also fall under the scope of the Cybercrime Convention which provides for criminal offences including the misuse of devices, i.e., the intentional production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing an illegal access or interception or a data or system interference. The sole possession of such devices might also constitute a criminal offence (Article 6 of the Cybercrime Convention).

Both the Cybercrime Convention and the Framework Decision 2005/222/JHA deal with the criminal liability of legal persons. Article 8 of the Framework Decision obliges each Member State "*to take the necessary measures to ensure that legal persons can be held liable for*

[88] See Article 22 para. 5 Cybercrime Convention.

offences referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on: (a) a power of representation of the legal person, or (b) an authority to take decisions on behalf of the legal person, or (c) an authority to exercise control within the legal person." It even goes further: "*a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority*." Article 9 contains specific penalties for legal persons.

Civil law and liability aspects

In the scenario, a number of other intermediary service providers are involved in the accident, such as the traffic light network provider. The company which has managed the traffic system had to guarantee that its system was sufficiently protected against hacking attacks. Since a minor was able to hack into the system, the protection was obviously insufficient. In a security breach like this, the company might be required to warn cars and buses that something is wrong. Did the company do enough in that respect?

It will be difficult to determine which of the various service providers involved in the traffic management system should be held responsible for the fact that a minor could break into the system. Normally, the victims would have to find the specific providers who did not provide sufficient protection and will have to prove that this provider committed a fault, which caused the specific damage. This is difficult to prove.

Article 1 and 4 of Directive 85/374 allow the victim only to prove that the traffic management system was defective. Since it was relatively easy to access the system, this condition might be fulfilled. This directive contains rules that allow the victim to react against the supplier of the defective good (or service), when the producer cannot be found. When the damage is caused by defects in the products or services of different suppliers, Article 5 makes it possible to claim all of the damage from one of the suppliers. This is important since it would be difficult for the victim to prove to what extent the different producers are responsible for the damages and to react against every single producer which is partly involved. As mentioned before, the directive is not applicable to services. This lacuna should be filled: a similar solution should be found for services.

Several service providers could be held liable for the damage caused by the security flaw. Directive 2000/31, however, limits the liability of intermediary service providers in three specific situations. Article 12 provides that "*Where an information society service is provided that consists of the transmission in a communication network of*

information provided by a recipient of the service, or the provision of access to a communication network, the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission."

Article 13 says "*Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.*"

Article 14 adds "*Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.*"

These provisions limit the responsibility only for the information transmitted. They will not be applicable when a system malfunctions because of a security flaw. Article 15 provides that the intermediary service providers have no general obligation to monitor the content of the information transmitted. This might be important in the sense that they cannot be held liable on the grounds that they should have noticed that damaging content was on the network.

The bus driver could be held co-responsible if it appears that he did not react appropriately.

The law applicable to the liability arising from the accident is

indicated by the Rome Convention on the law applicable to contractual obligations. A first important issue is that it only determines the applicable law in case of contractual obligations. The majority of issues in this scenario will have to be dealt with on the basis of national legislation. To determine the law applicable to the accident we have to distinguish various situations. When dealing with the liability of the hacker, we have an extra contractual liability. In this case, the national rules of private international law are applicable. When considering whether the company that provided the traffic managing systems is liable, we are dealing with both contractual and extra-contractual relations. The company of the traffic management system will have concluded directly or indirectly a contract with the bus company. If there is a direct contract between the bus company and the traffic management system company, we have to look at the Rome Convention. The parties to the contract can choose in the contract which law will be applicable (Article 3). If a choice has been made, it will often be imposed by the service supplier.

An important nuance, however, is this: "*The fact that the parties have chosen a foreign law shall not, where all the other elements relevant to the situation at the time of the choice are connected with one country only, prejudice the application of rules of the law at the country which cannot be derogated from by contract, hereinafter called 'mandatory rules'*" (Article 3 (3) of the Rome Convention). Thus, a service supplier cannot avoid the fact that the user will be able to enjoy the protection of some "mandatory rules". However, the criterion of the 'relevant elements of the case connected with one country only' makes this stipulation of limited utility in AmI, where we would frequently deal with the trans border situations. According to Article 4, even if the parties did not choose an applicable law in the contract, "*the contract shall be governed by the law of the country with which it is most closely connected (…).*" Article 4 further reads: "*…It shall be presumed that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporate, its central administration.*" In the instance of an AmI service supplier, he could have his habitual residence or central administration anywhere in the world and he could choose this place based on how beneficial the law is for him. Paragraph 3 of Article 4 contains specific rules for the carriage of goods. Similar specific rules could be created for the delivery of AmI services.

Regarding consumer contracts, specific rules exist for the delivery of goods and services. When the passenger wants to claim damages from the bus company we should look at Article 5 of the Rome Convention. This Article reiterates the principle that consumers cannot be deprived from their national consumer protection by the choice of law made in the contract. The consumer will enjoy the protection afforded to him

by the mandatory rules of the law of the country in which he has his habitual residence: "*(1) if in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all the steps necessary on his part for the conclusion of the contract, or (2) if the other party or his agent received the consumer's order in that country, or (3) if the contract is for the sale of goods and the consumer travelled from that country to another country and there gave his order, provided that the consumer's journey was arranged by the seller for the purpose of inducing the consumer to buy.*" Article 5, however, does not apply to a contract of carriage or to a contract for the supply of services where the services are to be supplied to the consumer exclusively in a country other than that in which he has his habitual residence. It shall, however, apply to a contract that, for an inclusive price, provides for a combination of travel and accommodation. This article is clearly built on the notion of habitual residence. In an AmI world, the notion of habitual residence might be flexible and this might make it difficult to apply these rules.

If the bus driver made a mistake, he might be liable towards his employer. Presumably both are situated in the same country – presumably Germany – and thus German law is applicable. If not, Article 6 of the Rome Convention contains specific rules on labour contracts.

The competent court in this case will be determined by Regulation 44/2001. As for the applicable law, the parties have the possibility to determine in their contract which court can be competent (Articles 23 and 24). Similar mechanisms are provided to ensure that certain "mandatory rules" remain applicable. The basis principle of this regulation is that "*persons domiciled in a Member State shall, whatever their nationality, be sued in the court of that Member State*" (Article 2). In case the defendant is domiciled outside the European Union, this regulation will not provide a solution for problems of jurisdiction (Article 4). We will have to look at national legislation. Although Article 2 sets out clear and important principles, it has disadvantage. When a user wants to sue an AmI services supplier, the service supplier will have the advantage of being sued at home. He might determine his domicile to ensure a beneficial jurisdiction. In addition to this general principle, the regulation contains a number of special jurisdiction rules, including those applicable to contracts, tort, and consumer and labour contracts. In matters relating to a contract, a person may be sued in the court of the place of the performance of the obligation in question (Article 5). In an AmI world, it will be difficult to determine the place of performance. In a certain sense, the contract is performed worldwide and this does not allow one to determine the competent court. Article 5 §1 (b) specifies that "*in case of the sale of goods [the place of the performance of the obligation in question shall be] the place in a Member State where, under the contract, the goods were delivered of should have been delivered …In case of the sale of*

services [the place of the performance of the obligation in question shall be] the place in a Member State where, under the contract, the services were provided or should have been provided". In case of a conflict between the bus company and the supplier of the traffic management system, the services – the traffic management system – had to be delivered in Germany, Italy and every place where they use the system. Thus, one cannot determine one single competent court. A similar problem exists concerning the contract between the bus company and its customers. The bus company provided and delivered services to its customers in Germany and in Italy.

The court competent to deal with extra-contractual issues, such as the liability of the hackers and the traffic management company towards the users, is the court of the place where the harmful event occurred or may occur. The European Court of Justice stated in the Bier Case (C 21/76) that the place where the harmful event occurred should be understood as the place where the damage occurred or the place where the event having the damage as its sequel occurred. In this scenario, the harmful event occurred in Italy, but the damage occurred not only in Italy, but also other places. The damage caused by the hacker is not limited to Italy. Hacking is a criminal offence and Article 5 § 4 provides that a civil claim for damage or restitution which is based on an act giving rise to criminal proceedings can be brought in the court seized of those criminal proceedings, to the extent that that the court has jurisdiction under its own law to entertain civil proceedings. Since several persons might be co-responsible for the accident, there could be several parallel proceedings. Since this would make the issue more complex and expensive for the parties, Article 6 provides that a person may also be sued "*where he is one of a number of defendants, in the courts for the place where any one of them is domiciled, provided the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.*" This allows the plaintiff to sue the different defendants before one single court. However, not all claims from the same factual situation may fulfil conditions set up by the Article 6. To offer an extra protection to the consumer, Article 16 of Regulation 44/2001 provides: "A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled." The bus customers can start proceedings in their own courts, which can be an important advantage. Specific jurisdiction rules are provided in case of individual employment contracts.

Conclusion

The definition of computer-related fraud does not completely fit the situation here. There can be no doubt that causing damage to others because of an intentional manipulation of a system should constitute a criminal offence. The definition might need to be clarified on this point. The Cybercrime Convention tries to realise this.

To determine the applicable jurisdiction in criminal affairs is still a complex affair, waiting for an international solution.

To determine the applicable jurisdiction in case of (extra-contractual) liability or tort, the national legislation applies. A uniform solution at European level would be preferable. A European instrument relating to those issues is now under the preparation.[89]

The provisions regarding contractual obligations and liability in the Rome Convention do not seem to be adequate to the Internet reality and even less to an AmI world.

6.2.2 Lack of interoperability

Situation description — A woman died because her health monitoring system was not compatible with the local (network health) system: Her injury was not detected.

Scenario link — "*What I did not know was that some passengers were using HMDs that are not compatible with the Italian system. Thus, they were not able to download the health information of a couple of people on the bus and the semi-automatic rescue co-ordination centre assumed there were only 32 people on board and sent too few ambulances. This did not have severe repercussions since many of us were not seriously hurt.*"

Legal field — ICT law – Standards and operability - Liability – discrimination

Legal chapter — Directive 98/34 on technical standards and technical regulations in Information Society Services – Directive 85/347 concerning liability for defective products – Directive 91/250 on the legal protection of software – Directive 2002/22 on universal service and user's rights relating to electronic communications networks and services.

Discussion — The health monitoring system did not work because it was not compatible with the Italian system. In an AmI world, interoperability is crucial.

To ensure that information society systems and networks are compatible, international standards are created. The European Commission and international and European standardisation bodies are active in this domain. An important legal instrument to ensure the creation of uniform standards and technical regulations is Directive 89/34 which regulates some aspects of standardisation in the European Union. It provides that national authorities and the European

[89] Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations ("Rome II")COM (2003) 427(01)

Commission should inform each other about new initiatives in the field of technical standards and norms (Articles 2 to 4). This should guarantee the necessary level of transparency between the different competent bodies in the European Union. The directive also provides for the establishment of a standing committee, consisting of representatives appointed by the Member States and, as chairman, a representative of the Commission. This Committee should be consulted by the European Commission in case of new initiatives and ensures that the national interests of Member States are taken into consideration.

Member States also have the obligation to ensure that their standardisation bodies do not take any action that could prejudice European standardisation initiatives. When a Member State wants to create new technical regulations, Articles 8 and 9 provide detailed information and co-operation procedures, to ensure compatibility with European Union and other national initiatives.

All of this should guarantee that the European Commission and the Member States work together in the most efficient way and are aware of each other's initiatives. If it were to work optimally, all national systems should interoperate and be based on compatible standards and regulations. Similar standardisation initiatives exist at the international level.

Regarding the important (and for AmI necessary) interoperability of software programs, one can refer to the Software Directive of 1991, which contains a provision on interoperability in order to avoid a situation where copyright could hinder interoperability. It states in Article 6 ("Decompilation") that the authorisation of the rights holder shall not be required where reproduction of the code and translation of its form are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met: (a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so; (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and (c) these acts are confined to the parts of the original program which are necessary to achieve interoperability. These provisions "*shall not permit the information obtained through its application: (a) to be used for goals other than to achieve the interoperability of the independently created computer program; (b) to be given to others, except when necessary for the interoperability of the independently created computer program; or (c) to be used for the development, production or marketing of a*

[90] Rb. Leeuwarden 25 May 2005 Openbaar onderwijs Zwolle/Pendula, available at http://www.rechtspraak.nl.
[91] http://europa.eu.int/comm/internal_market/copyright/docs/docs/fordham2005_en.pdf

computer program substantially similar in its expression, or for any other act which infringes copyright.[3] *In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the right holder's legitimate interests or conflicts with a normal exploitation of the computer program.*"

There has not been much case law based on the directive. A Dutch court, however, recently decided that the Dutch copyright law (implementing the Software Directive) obliges application service providers to copy the data, which are processed in one program, to a script that makes it possible to process the same data in another program. In this case, a school wanted to change the software program without losing the data, and the Court decided that the first software provider (application server provider) was obliged to make a script that translates the data into the other program.[90]

There have been many criticisms of this judgement because the Software Directive indeed had foreseen the interoperability of software, not the interoperability of data. But this exactly highlights an interesting issue for AmI: To what extent are licensors of software programs compelled to deliver the data, processed in their programs, in a script that allows processing the data in another program? This is of particular importance for the data subjects who have according to article 12 an access right to the data, namely a right to communication "*in an intelligible form of the data undergoing processing and of any available information as to their source*". This is also important for anyone who needs to use (personal) data and other information processed in any other processing system.

Tilman Lueder, acting head of the Copyright Unit - DG Internal Market and Services, announced that the Commission will make an impact assessment to determine "whether the Software Directive's provisions on interoperability are sufficient to ensure that new business or software development models can thrive in the EU."[91] Another case that relates to interoperability is the Commission Decision of 24 March 2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft) in which the Commission decided that on the basis of article 82, Microsoft abused its dominant position "by deliberately restricting interoperability between Windows PCs and non-Microsoft work group servers, and by tying its Windows Media Player (WMP), a product where it faced competition, with its ubiquitous Windows operating system." The Commission imposed a fine of € 497 million and the following remedies on Microsoft: (1) the obligation to offer an unbundled version of Windows (a version of Windows without Windows Media Player) ("unbundling of WMP" remedy); (2) the obligation to make available to its competitors certain technical interface information necessary to allow non-Microsoft work group

servers to achieve full interoperability with Windows PCs; this having to be done on reasonable and non-discriminatory terms ("interoperability remedy"). However, this case is now pending before the ECJ. Such and similar, specific interoperability remedies might be necessary in AmI. Lack of interoperability can not only preclude individuals from obtaining the services they wish to enjoy, but can also result in serious damage caused to them, as shown in the scenario.

There is no doubt that the technology can facilitate life of the individuals. Well functioning emergency systems may safe lives. On the other hand, creating standards has a cost. Question arises who will bare the costs of such developments. Companies might be less willing to contribute to the development of standards because they will not receive the expected return on investment on the one hand, while they still might be liable for the good functioning of their standardized product on the other hand. In the example from the scenario, the woman was not provided with the compatible device. Universal Service Directive 2002/22 recognised the need of providing the universal services to end-users at an affordable price. However, the scope of the Directive is limited to the electronic communication networks and services and very few services. It would be desirable to examine new emerging AmI services and technologies against the need to provide these services and technologies to all individuals in a non-discriminatory, reasonable and safe way.

Conclusion

The issue of standardisation and interoperability is of major importance for AmI applications in the information society. When standards have been achieved, stringent regulations should be imposed, at least to very sensitive AmI services such as health and general alarm systems, to ensure compliance with the standards and regulations throughout the EU.

Even in the hypothesis of a worldwide agreement on certain standards, however, people still will need to be able to afford the technology based on these standards. In this scenario, the insurance company refuses because it considers it to be too expensive. In more extreme situations, a whole country or continent may not be able to afford these technologies. This highlights the issues of affordability and discrimination, which may be reinforced by introducing new and costly technologies. Sensitive AmI services and technologies could be treated as public or universal services, which should be available to all. The topic is high on the European agenda. There have been research activities relating to accessibility, under the eEurope 2002 action plan. The Council also adopted a resolution on e-accessibility in December 2002. The eEurope 2005 action plan will seek to ensure that people with disabilities and other disadvantaged groups can participate in and have equal access to major innovations in on-line public services, covering e-government, e-learning and e-health, and also to create a dynamic, accessible e-business environment.

6.2.3 *Access refusal as a result of data mismatch*

Situation description	Person refused transport because of problems with identification
Scenario link	*"Michael from Baden-Baden was denied access to the boarding area of the terminal, although he had a valid ticket and even could present the receipt from his travel agent!*[92] *Apparently, some kind of data mismatch between his personal ID, the e-ticket and the information stored on the central server had caused the problem. The security personnel at the terminal were absolutely stubborn and unwilling to make an exception, despite several interventions by Alessandra and Peter, who, by the way, is a good friend of Michael."*
Legal field	Privacy and Data Protection (first and third pillar) – Identification – Biometrics
Legal chapter	Data Protection Directive 95/46
Discussion	In the AmI world, new tools and methods for identification will be developed, manufactured and implemented. In the scenario, the public transport relies on biometric identification. No identification system, however, is perfect; each is subject to errors to a greater or lesser extent. The data controller takes the risk for and bears (some of) the consequences of the errors. Today, errors seem to be accepted as a fact of life, however undesirable, as they can cause harm to people, especially when identification systems become much more prevalent than they are today. The problem spotlighted by this scenario is caused by a mismatch between the personal data and the data and other information held on a central server. We do not know why such an incompatibility of information occurred. The information on the central server has been collected, acquired and processed under the responsibility of the data controller of the l server. The data controller is responsible for matching the personal data. Article 17 of the Directive 95/46/EC determines that "*the data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected*." A mismatch does not automatically imply destruction, loss, alteration (there is no alteration if the personal data of Michael from Baden-

[92] Schneier, B., 2004.

Baden have been changed after they were stored on the server), unauthorised disclosure or access. So it is difficult to find protection in the security and confidentiality obligations of the Directive 95/46 (and 2002/58, see below).

The directive also requires information collected to be accurate and up-to-date. Compliance with those requirements can be treated as important protection of the data subject's privacy. Correctness of the processed data is obviously crucial. A similar obligation is provided in article 4 of Directive 2002/58. Be that as it may, however, the obligation to keep personal data accurate and up-to-date is difficult to achieve in an AmI world where the accuracy of the processing depends mainly on the accuracy of the data processed. The mismatch in this case could be a consequence of an update of Michael's personal data that occurred just an hour before. Also, for reasons of interoperability, mismatching might increase fundamentally in AmI. Mismatching as a consequence of a lack of interoperability lies outside the responsibility of particular data controllers. Indeed, the scenario shows that the data controller tries to avoid any responsibility and puts the burden on the users of the system.

Refusal to provide the service (to Michael) may also be the consequence of defective services, hardware or software. It causes damage to the data subject. Who is liable for such damage? In the scenario, the security personnel try to eliminate their liability for the damage caused by shifting the liability to the group. There is no justification for doing so, since the problem was not caused by the group, or by Michael, and may well have been the result of an error in the central server of the security service itself. Article 12 of Directive 85/347/EC repeats an important principle of tort law: "The liability of the producer of a defective product (the security control system) may not, in relation to the injured person, be limited or excluded by a provision limiting his liability or exempting him from liability." The directive may provide the grounds for Michael's claiming damages if he had been refused and not permitted to participate in the trip, and if the refusal had been caused by a malfunction of the server.

Conclusion

Policy-makers should provide for a system that creates a well-organised, fast and effective right to object to the erroneous interpretation or processing of personal data, as well as a tool for immediate compensation when access has been denied. It could be also examined whether the access should not be denied in case of some basic and essential services on the ground that the person has the problems with identification (for example if Michael would be refused on the public transport system). Such deny of access can be discriminatory, when it occurs due to error in profiling the data or lack of the data.

6.2.4 Disproportional request for personal information

Situation description

A hospital requires mandatory access to the complete medical record of a slightly injured patient, but such access is disproportionate. When the patient refuses to give such access to his complete record, he is obliged to sign a statement waiving the hospital of any liability for any impairment from the treatment.

Scenario link

"After we arrived at the hospital, I had a fierce argument with the lady at the reception who complained that she was not able to access my health and insurance record completely. The doctors, she said, were unable to help me if I wouldn't disclose my complete data to the hospital. (…)I saw no necessity to give the hospital complete access since I only had some scratches. However, I had to sign a statement that the hospital is not liable for any impairment resulting from their treatment.

Legal field

Privacy and data protection – consumer protection law –

Legal chapter

Data Protection Directive 95/46 – Directive 93/13 on unfair terms in consumer contracts.

Discussion

This part of the scenario highlights two major problems of data protection in AmI. First, the principle of "proportionality" (a cornerstone of data protection law) is questioned. Second, the concept of "consent" and how consent takes place should be examined in the context of AmI, which may curtail our freedom of choice in many situations.

The Data Protection Directive 95/46 and other data protection regulation repeats the principle of proportionality, laid down in the first internationally binding document regarding data protection, namely Treaty 108 of the Council of Europe (1981). The principle of proportionality in Directive 95/46 states that "*the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.*"

Despite its importance, this principle risks being eroded in a fast society with constant data processing and systems capable of intelligent processing and using large amounts of personal data. In other words, disproportionate data processing often takes place. There is not much case law in which one can find out what "proportional" data processing is and what isn't. In addition, it is very difficult to define what is "proportional". On the one hand, there are too many diverse situations in which processing takes place, so that one particular situation might require more data processing for one reason or another. On the other hand, a definition of what is proportional and what is not somehow takes away the right of an individual to decide himself who has access to his personal data, who can access them and how long they may be stored. Some persons might even find

advantages in a vast and extensive processing and storage of their personal data.

Data protection officers don't often use the possibility to check the proportional character of data processing by data controllers. There is too much data processing taking place in AmI in order to effectively control data controllers. In addition, many data controllers are exempted from notification of the processing to the data protection office, so that no *a priori* control of the data controller can take place.

This brings us to the second issue, which is that of the consent of the data subject: Processing of personal data must be "legitimate". This is stated explicitly in article 7 of the directive. Beyond a series of exceptions that we will not address here (processing necessary for the performance of a contract; or for compliance with a legal obligation to which the controller is subject; or in order to protect the vital interests of the data subject), legitimacy is based on three general principles.

The first concerns processing operations to help fulfil government tasks and pursue the public interest by the authorities themselves or others working for them. Government data processing has to meet the criteria of the judicial framework of the specific administrative authority and comply with its statutory powers. On top of that, each action by the authorities has to meet the criteria of the public interest. Mutatis mutandis, this also applies to the processing operations that the authorities manage or delegate. As a result, government data processing is not justified when it is not necessary for the exercise of a specific power of the administration concerned. It is just as unjustified when government data processing operations constitute a disproportionate invasion of privacy, since protection of privacy is, to a great extent, part of the public interest. There should be less invasive methods available to achieve the same goal. In addition, government data processing has to respect Article 8 of the ECHR. The restrictions set out in the second paragraph of that article fully apply. And apart from the aforementioned legitimacy and proportionality requirement, government data processing must be necessary in a democracy and be "*in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or the protection of the rights and freedoms of others.*" Since personal data processing runs by definition counter to privacy, it implies that it will only be legitimate when it contributes to the realisation of one or more of the goals set out in the second paragraph of Article 8. So the processing operation is not justified simply because it is executed by or for the government. National rules need to make this meticulously clear. They have to ensure and encourage that the judges and the specially-created supervisory authorities consider the interests of every side in every situation.

A second legitimacy principle primarily concerns private processing

of personal data. Article 7(f) of the Directive says that *"processing is necessary for the purposes of the legitimate interests pursued by private interests, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."* Again two aspects intertwine. In the first place, the ultimate purpose of the processing should be lawful. An illegal or illegitimate interest can never be pursued by a legitimate processing operation. If the processing is undertaken by a legal person, its corporate purposes will be taken into account as an additional touchstone. Legal persons can only undertake action to achieve the goals laid out in their articles of association. The processing operation has to seamlessly fit in that concept. Second, the processing operation must be clearly necessary and indispensable to achieve the set purpose of the processor. Is it possible to achieve that purpose through other means? In regard to privacy, is this the least harmful way? Proportionality and subsidiarity are essential. The interests have to be carefully balanced, taking into account their hierarchal entrenchment and the necessary catch-up operation to safeguard privacy. In each case, the concrete interests facing each other have to be carefully evaluated. A purely commercial purpose which results in a drastic invasion of privacy (e.g., the processing of personal data for direct marketing sales) has to be judged differently (and more severely) than data processing necessary to maintain public health, freedom of speech or, for that matter, the running of a sports club.

The third legitimacy principle is consent. Article 7 (a) states that "*personal data may be processed only if the data subject has unambiguously given his consent.*" Consent is taken to mean "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*" (Article 2 (h)).

Processing personal data is thus justified if the data subject clearly gives his/her consent after being informed of all aspects of the processing operation: the delineated and justified purpose of the processing operation, the categories of personal data which will be processed, possible third parties which will have access to the information, who is responsible, his/her rights, etc. The un-ambiguity and specificity of the consent and the complete information on which it is based will need to be proved by the processor in case of conflict.

The consent criterion engenders a number of difficulties. First, the freedom of choice is in practice often a limited and relative one. Not everyone in our society has the same freedoms and possibilities. It may be an objective, but it is not a reality. Most personal data processing creates a relationship in which the data subject is the weak party in the balance of power. The behaviour of a data subject is steered; the data flow is often one-way. Most of the time, the data subject needs something (e.g., credit, health insurance) and is almost forced to give consent. In the end, consent is often turned into a pure

formality without offering any guarantee. Just think of entry contracts and their clauses. Second, the general framework of the directive leaves it unclear what processing operations can be justified solely based on the consent of the data subject. If no consent is given, the other legitimacy grounds in themselves seem to span the whole gamut of possibilities. Unless one assumes that such consent legitimises disproportionate and illegitimate processing – which is questionable. It is tough to invoke the consent of a data subject in order to legitimise a totally disproportionate invasion of privacy. In penal law, the consent of a victim does not erase the criminal character of an action. Mandatory secrecy is not affected when a party gives consent to make something public. The mutual consent between parties on illegal agreements does not yield a legal agreement. As a result, the unambiguous consent of the data subjects is only one of the aspects that affect the considerations of the different interests. Finally, it is well advised that the withdrawal of consent should be explicitly mentioned in legislation.

In the case sensitive personal data, such as health-related data, things are even more complex because the Data Protection Directive has created a special regime. Indeed, Member States must *proscribe* the processing of "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*" (Article 8 (1) of the Data Protection Directive). In those cases, a fundamental data processing prohibition applies because it endangers not only privacy, but also the principle of non-discrimination. Yet this fundamental ban also allows for exemptions. For example, Article 8. 4 of the Data Protection Directive states that "*subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions.*" There is even provision for an exemption if the data subject has given "explicit consent" to the processing of such information. The hospital example shows that this consent is often not freely given because the data subject is in a subordinate situation. He is subject to the power of the data processor and controller, who possess a good or a service one wants. In this scenario, the data subject is dependent on the hospital (and therefore will mostly give disproportional access to his personal data), but also the hospital is dependent on the insurance companies that require hospitals to enforce access to the complete records of their patients (and therefore the hospitals will mostly ask disproportional access to the personal data).

The non- discrimination principle is well established in the European Law.
Articles 21 and 23 of the Charter of Fundamental Rights of the European Union prohibit discriminations based on grounds such as sex, race, color, nationality, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or

sexual orientation. The non-discrimination principle has its place also in the Treaties (Article 6 of the Treaty on European Union, Articles 7, 12 and 13 of the Treaty establishing European Community) and in the large scope of the legislation implementing those provisions. However, the enforcement of this principle may require further limitation of the processing of data in respect of the non-discrimination criteria (for instance the processing the data relating to health by insurance companies), and exceptions must be very carefully established.

Conclusion Disproportionate data collection is prohibited. This principle, however, can conflict with AmI environments in which, on the one hand, the environment needs to process as much data as possible (because there is a need for so much personal data, the processing can not be disproportional) and, on the other hand, the data subject might accept this processing of data in a disproportional way.

6.3 SCENARIO 3: CORPORATE BOARDROOM & COURT CASE

6.3.1 Global companies and local laws

Situation description The Data Mining Company (DMC) is active in Europe, the US and Asia.

Scenario link *"It is headquartered in Miami, but now has major subsidiaries in London and Tokyo. It is listed on the New York and London Stock Exchanges and is considering a listing on the Tokyo Stock Exchange."*

Legal field Private international law – Privacy – Data Protection – Transfer to third countries – Safe Harbour Principle

Legal chapter Data Protection Directive 95/46/EC – Convention of Rome on the Law Applicable to Contractual Obligations – Regulation 44/2001 on jurisdiction, recognition and enforcement of judgements in the civil and commercial matters

Discussion DMC is active around the world. An important question is which law will be applicable to which data collector and to which data processing. Is the EU Data Protection Directive 95/46 applicable outside the EU? A second issue relates to the special provisions of the directive concerning the transfer of personal data to third countries outside the EU.

The first question is solved by Article 4 of Directive 95/46 which determines that the national law of the Member States will apply where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. This provision is not clear. It may lead to the application of the law of

the Member State where the data controller is established, if processing is carried out in connection with this establishment. Such requirement may often be fulfilled; even if we are not sure where the processing of data as such took place (collecting the data may also be understood as such contexts). It may lead, however, to the application of many laws since most likely the data processor will be established in many states. Article 4 further stipulates that if the data controller is established on the territory of several Member States, he must ensure that each of those establishments complies with the obligations laid down by the law applicable. DMC has establishments in the United Kingdom, Japan and the United States. Article 4 (c) determines that if the controller is not established on Community territory the national legislation of a Member State of the European Union will apply when the processor, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community. DMC could try to prove that the equipment in the United Kingdom is only used to transmit information to the United States or Japan, thus preventing the use of the Community legislation.

The personal data, the information and the profiles, deduced and extracted from these personal data, are processed, transferred, licensed and otherwise traded on a worldwide level with hundreds of unknown clients. DMC grew through mergers and acquisitions and processes data (of European citizens) in many countries outside the EU.

As regards the second issue, article 25 of Directive 95/46 states the following: "*The transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. Where the Commission finds that a third country does not ensure an adequate level of protection, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question. The Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.*"

In execution of this article, the European Commission has concluded the "Safe Harbour Agreement" with the US, which aims to ensure the protection of personal data transferred from European Member States to the US. Organisations that wish to obtain and maintain recognition of the fact that they ensure an adequate level of protection must subscribe to the principles provided in the agreement, reveal their confidentiality rules and fall within the competence of the Federal Trade Commission (or of any other body fulfilling a similar mission). When DMC transfers data from the EU to companies in the United States, it must thus ensure that these companies have subscribed to the Safe Harbour Agreement. The European Commission decided in decision 2000/520/EC (Commission Decision of 26 July 2000) that the "Safe Harbour Privacy Principles" are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States.

The Commission also decided that Argentina (Commission Decision C(2003) 1731), Canada (Commission Decision 2002/2/EC)[93] and Switzerland (2000/518/EC) provide an adequate level of protection for personal data transferred from the Community to those countries. The Commission is currently looking into the privacy protection schemes in New Zealand, Australia and Hong Kong. Only a limited number of countries have received such recognition. Transfer to African and other developing countries could pose problems, since they probably do not provide an adequate level of protection.

Article 26 provides for an exception: "*A transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection, may take place on condition that: (a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case."* These conditions are clearly not fulfilled in this scenario. *"A transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection may*

[93] There are however some discussions whether Canada offers an adequate protection.

also be authorized where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses." In these last two cases, the Member State has to give permission, which DMC does not seem to have acquired.

Conclusion When data is collected from EU citizens, it is in their interest that EU law remains applicable. Data subjects should not lose the protection of their national legislation when the data collector, processor and /or controller transfer the information outside the European Union, and doesn't establish himself on the EU territory. That is why it might be better to determine the applicable law on the basis of the place of establishment or the domicile of the data subject or the place where the data are collected. In an AmI world, it will become increasingly difficult to determine "where" data are processed or collected. The criterion of the place of establishment or the domicile of the data subject may also have the advantage of preventing the forum selection by the data processor who is now free to choose the most liberal legal regime to establish himself.

6.3.2 Monitoring of employees

Situation description The employees at the workplace are continuously monitored.

Scenario link *"The boardroom video screen switches from the agenda and shows MacDonald's office. He is heard and seen finishing off a conversation with a journalist. He gets up from his desk and leaves his office. As he does so, another camera in the hallway shows him going down a corridor…"*

"Surely you can track them [the employees] via their location implants. Everybody has to have a location implant. It's a condition of employment in our company, just like any critical infrastructure like banks, nuclear power companies, etc."

Legal field Privacy and Data protection (at the workplace)

Legal chapter Article 8 of the ECHR – Data Protection Directive 95/46

Discussion Vice-president MacDonald is monitored the whole time. What would happen if he were doing something private, such as calling his children? It seems that all recorded data are stored (for how long?).

As explained in section 6.1.1, people do not lose their privacy in an office or professional environment. Even so, in an AmI world, the division between the private and office spheres will become more blurred. Until now, the Court of Strasbourg has not decided a case of

permanent monitoring in the workplace and it is unsure whether such monitoring will be found in accordance with Article 8 ECHR. Monitoring systems (like bio location implants) that allow a permanent monitoring, even when one is not working (for example, to trace somebody who violates the security obligations), will likely be found incompatible with Article 8 ECHR, which not only protects the private life but also her/his family life and home. Professional location implants that enable monitoring of an individual's behaviour at home and in one's private and family life will most probably be refused.

Additional arguments for this reasoning can be drawn from the Data Protection Directive prohibiting excessive processing of data and prohibiting as a rule the processing of sensitive data. Permanent monitoring will reveal such data, e.g., the subject's going to certain hospitals or to sensitive locations such as churches or political meetings.

There seems to be no margin of negotiation if you want to be employed by DMC. Also, the so-called consent which is given in the contract must be viewed in the light of Article 7 of Data Protection Directive 95/46/EC which provides that personal data may only be processed if the data subject has unambiguously given his consent. In this case, it could be argued that employees were forced to give their consent – i.e., if they wanted to work at DMC, they are forced to consent, which, of course, is not consent at all. The processing can be justified when it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. DMC could argue that the data processing is necessary as part of the labour contract.

DMC needs to be sure that confidentiality is respected. Article 7 (f) also provides that the processing can be allowed when it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject. There needs to be a balance between the legitimate interests of DMC and the fundamental rights and freedoms of the employees, such as the right to privacy.

The data are collected for a specific purpose, to ensure the confidentiality and business interests of the company (Article 6 b). The information obtained via the location implants could be used for totally different purposes. Since DMC is a real data mining company, it might use location implants to collect as much information as possible. This could happen without the consent of the employees or for purposes which were not previously agreed. There seems to be a problem with the principle of proportionality.

Belgium's Collective Labour Agreement no. 81 of 16 June 1998 explicitly foresees a prohibition on permanent monitoring of

employees. This Agreement was conceived as an additional tool to strengthen the existing Belgian data protection law of 1992, amended in 1998 to implement the Data Protection Directive. There exists no harmonisation in this field, which clearly is needed.

Conclusion The case of permanent monitoring will probably provoke a lot of reactions in the future. Although there is no general prohibition against it, there is enough ground to assume that it will not get through as a general rule or practice in the next decades, with the possible exception of certain groups, such as prisoners and children.

6.3.3 Global interoperability

Situation description AmI does not cover the whole world. Some countries use older systems and this creates problems of interoperability. Other countries do not (intentionally or not) co-operate in the creation of an AmI world or, on the contrary, are forced to co-operate.

Scenario link *"Unfortunately, most developing countries have no AmI networks, which makes it impossible to build up the same kind of detailed profiles of individuals like we can here in the US, Europe or Japan. So the immigration authorities have been making threatening noises about refusing entry to people from countries without AmI networks."*

Legal field Interoperability

Legal chapter Directive 98/34 laying down a procedure for the provision of information in the field of technical standards and regulations

Discussion We here refer again to section 6.2.2.

Even within EU countries, interoperability is of major importance. Directive 98/34 provides a co-operation and information procedure in order to ensure that the European Commission and the national standardisation bodies work together. This should ensure that the national standards and technical regulations of the different Member States are compatible and enhance efforts to create European standards. At an international level, similar standardisation initiatives have been and are being undertaken. Some countries cannot afford internationally recognised technology.

This is, however, only one aspect of the problem. A fully operational generalised interoperable AmI world would be a threat for a whole range of fundamental rights such as privacy, non-discrimination, free movement, the right to anonymity, etc.

Conclusion Use of the same technical standards and regulations worldwide would solve the problem of interoperability. The majority of those standards are created in the developed world and in many domains, it is

expensive to comply. Developing countries, as mentioned in the scenario, may not be able to afford these technologies and to have compatible technology. To ensure maximum interoperability, initiatives are needed beyond those aimed at the creation of common standards. Countries should also have the possibility to develop the necessary infrastructure to comply with them.

Governments could fundamentally contribute to the development of good standards by increasing technical regulations, by financing and co-operating in research that leads to standards, and by imposing taxes on non-standardised goods and services.

6.3.4 Trading of personal data and role of data subject

Situation description Trading of personal data and databases, storage of incorrect data and the difficulty confronting the individual to correct the information.

Scenario link "*…(DMC) has actually been selling large chunks of it to governments and to other companies who in turn were using the data to spam just about everybody in the United States and here in the UK too.*"

"*Questions have also been raised about the accuracy of the data. People are entitled to see their records, but most people didn't even know about DMC, let alone the fact that they had built up such extensive records on every one of us.*"

"*We heard that in many instances the information was wrong, that the data coming from so many different ambient technology networks were often in conflict or didn't make any sense.*"

"*… some of that data, as you know, has not always come from legitimate sources.*"

"*Some witnesses said they had been trying to get wrong information cleaned from their records for almost two years, and have yet to succeed.*"

Legal field Privacy & data protection

Legal chapter Data Protection Directive 95/46

Discussion This situation is clearly related to data laundering, which has already been discussed in section 6.1.8 above. DMC is active in exchanging and trading personal data with other companies and with the customs authorities. It tries to keep a low profile, so that its activities do not become known to a wider public. DMC grew through mergers and acquisitions. The data collectors, from whom they (presumably sometimes illegally) obtained the personal data, often do not exist any more.

The data sold were often misused for spam and different other types of fraud. All of this seems to imply that they do not respect the fundamental data protection principles as expressed in the Directives 95/46/EC and 2002/58. DMC aims to maximise its revenues from this information. It collects excessive amounts of personal data and builds excessive profiles about the data subjects to whom they are applied by one of the numerous clients of DMC.

The information collected by DMC appears to be inaccurate or incomplete. Also at the first level of the collection of the personal data (before DMC acquires them and processes them into profiles), data controllers have the obligation on the basis of Article 10 of Directive 95/46/EC to inform the data subjects of any processing of their data, and to inform them about the purposes of the processing, especially the transmission of personal data to third parties.

Any further information such as the recipients or categories of recipients of the data, the existence of the right of access to and the right to rectify their data is only required *"in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected to guarantee fair processing in respect of the data subject"*.

When personal data are disclosed to third parties, Article 11 ("Information where the data have not been obtained from the data subject") provides that the controller or his representative must, no later than at the time when the data are first disclosed, provide the data subject with at least the following information, except where he already has it: *"(a) the identity of the controller and of his representative; (b) the purposes of the processing; (c) any further information such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.*"

It must also be said that, if the personal data are made anonymous before they were received by DMC, data protection law does not apply to the processing of the anonymous data by DMC. Of course, the act of anonymising data is a processing that falls under the Data Protection Directive 95/46, but if this occurs by other data controllers before DMC receives the anonymous data, DMC is not bound by the national provisions that implement Directive 95/46.

Conclusion

Companies that process personal data acquired from third parties are bound by the rules of data protection. It might be a good safeguard to oblige those companies to check where the information they buy comes from and if it has been lawfully acquired. Similar obligations

could be imposed like those on banks to control money laundering.

6.3.5 *IPR and personal profiles*

Situation description	DMC owns all intellectual property rights in its databases and in its profiles, built upon (anonymous or identifiable) personal data.
Scenario link	The databases owned by DMC and other companies are protected by intellectual property rights.
Legal field	Intellectual Property Rights
Legal chapter	Directive 96/9 on the legal protection of databases
Discussion	The databases owned by DMC and other companies are protected by intellectual property rights. Directive 96/9/EC provides a copyright protection for the selection or arrangement of the content of the database and a *sui generis* right for the content of the database. In the case of the DMC databases, the selection or arrangement will be important, since DMC tries to create profiles and adapt services on the basis of the information collected. DMC, as an author of the database, will have the exclusive right to carry out or to authorise: "*(a) temporary or permanent reproduction by any means and in any form, in whole or in part; (b) translation, adaptation, arrangement and any other alteration; (c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community; (d) any communication, display or performance to the public; (e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b)*" (Article 5). In an AmI world, service providers will use massive databases and they will not only use the content, but also the structure or selection or arrangement of the database. The protection offered is extensive and it is impossible to require every time permission to reproduce, translate and/or communicate it. Article 6 provides for some exceptions to the exclusive right of the author: "*The performance by the lawful user of a database or of a copy thereof of any of the acts listed in Article 5 which is necessary for the purposes of access to the contents of the databases and normal use of the contents by the lawful user shall not require the authorization of the author of the database.*" It is unclear what should be understood by "lawful user". Depending on the interpretation, it could limit the scope of the exception to a greater or lesser extent. The second paragraph provides for a number of optional exceptions. Limitations on the rights set out in Article 5 can be provided in the following cases: "*(a) in the case of reproduction for private purposes of a non-electronic database; (b) where there is use for the sole purpose of illustration for teaching or scientific research,*

as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved; (c) where there is use for the purposes of public security for the purposes of an administrative or judicial procedure."

The content of the database is protected by a *sui generis* right. In order to obtain this *sui generis* protection, the maker of the database has to show that "*there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.*" The terms extraction and re-utilisation are defined in a broad way (Article 6).

The fourth paragraph of Article 6 states clearly that the *sui generis* protection shall apply irrespective of the eligibility of the contents of that database for protection by copyright and by other rights. This implies that the maker can obtain the *sui generis* protection, even when the content consists of personal data. Although the user does not have a property right over his personal data, the maker of a personal database can obtain an exclusive right over this type of data. Article 8 gives the lawful users of a database the right, when the database is made available to the public in whatever manner, to extract and/or re-utilise insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. There are limits to this right: he may not perform acts which conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database and may not cause prejudice to the holder of a copyright or related right in respect of the works or subject matter contained in the database.

Article 9 provides a number of optional exceptions to the *sui generis* right: "*The lawful users of a database which is made available to the public in whatever manner may, without the authorization of its maker, extract or re-utilize a substantial part of its contents: (a) in the case of extraction for private purposes of the contents of a non-electronic database; (b) in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved; (c) in the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure*". Certain exceptions to the exclusive right of the maker of the database are thus provided, but they can only be used by the "lawful users" and, especially, by the lawful user of a database which is made available to the public. Consequently, for example in the case of profiling, these exceptions are rather limited or even non-existing. The right to use freely publicly available databases might contradict with the right to privacy which prohibits the owners of databases to make them public. In an AmI world where massive amounts of information and databases will be exchanged and traded, the

protection of databases might thus put a burden on free trade.

Conclusion Compared to the exclusive rights provided to the author or maker of the database, the exceptions are rather limited and do not provide a solution to the fact that service suppliers will not be able to ask the author of the database for permission every time. Databases containing addresses, locations, weather information, sports results, pollen information, medical data… they all need to be coupled and need to co-operate to make AmI work. This is not possible in an intellectual property right system where copyright and database owners impose unreasonable prices, limit competition and make exclusive contracts with one company (excluding the other). Making databases available to the public may be difficult to reconcile with privacy and data protection law.

6.3.6 Data theft

Situation description Hacking of servers and data theft. An unknown person has hacked the servers and has stolen (or copied) information.

Scenario link "*…DMC discovered that someone had broken into its supercomputers and copied data on a lot of people. For a few weeks, DMC didn't say anything to anybody…*"[94]

Legal field Criminal law – Privacy & security – Identity theft – Data protection

Legal chapter Cybercrime Convention – Framework Decision 2005/222/JHA

Discussion The persons who broke into the DMC servers committed criminal offences as defined in the Cybercrime Convention, such as illegal access, illegal interception, data and system interference, possibly misuse of devices, computer-related forgery and computer-related fraud. The Cybercrime Convention provides a common definition of crimes for all the contracting parties and for procedural rules to react to these crimes. The protection offered by this convention is quite broad, since it also considers as a criminal offence the intentionally aiding or abetting or attempting the commission of the above-mentioned crimes (Article 11). The Cybercrime Convention also provides as criminal offences the misuses of devices, which is "*when committed intentionally and without right (a) the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing an illegal access or interception or a data or system interference.*"

[94] See Krim, Jonathan, "Consumers Not Told Of Security Breaches, Data Brokers Admit", *The Washington Post*, 14 April 2005.

The sole possession might constitute a criminal offence (Article 6 of the Cybercrime Convention). The Cybercrime Convention and the Framework Decision 2005/222/JHA deal both with the liability of legal persons. Article 8 of the Framework Decision obliges each Member State "*to take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on: (a) a power of representation of the legal person, or (b) an authority to take decisions on behalf of the legal person, or (c) an authority to exercise control within the legal person.*" It even goes further: "*a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority.*" Article 9 contains specific penalties for legal persons.

Conclusion When it comes to establishing the criminal liability of individuals, serious problems can occur when the degree of intent required by the legal provisions must be proven.

6.4 SCENARIO 4: RISK SOCIETY

6.4.1 Personal profiling

Situation description Personal profiling is increasing and can influence individual decisions.

Scenario link *"I think a lot of people simply do not realise how much personal information they are constantly giving out.*[95] *APPAG wants to raise public awareness about this issue and wants to warn people that personalised profiling is simply too risky."*

Legal field Privacy and data protection – E-commerce

Legal chapter Data Protection Directive 95/46/EC – E-commerce Directive 2000/31 Privacy & Electronic Communications Directive 2002/58

Discussion Service providers collect huge amounts of information and share it with other companies to be able to offer more personalised services. People are not aware of the data which are transferred and exchanged between companies. There is a substantial risk that this personal profiling is manipulated.

[95] Tuohey, Jasey, "Government Uses Color Laser Printer Technology to Track Documents. Practice embeds hidden, traceable data in every page printed", 22 November 2004. http://www.pcworld.com/news/article/0,aid,118664,00.asp. See also Jardin, Xeni, "Your Identity, Open to All", *Wired News*, 6 May 2005. http://www.wired.com/news/privacy/0,1848,67407,00.html

Here again, the data protection rules apply. Personal data must be collected and processed for a specific purpose (article 6 (c) of Directive 95/46/EC). First, when a profile is built upon personal data, data protection law applies whether the profile is an individual profile (related to an identifiable person) or a group profile (built with anonymous data). Making the personal data anonymous is a processing that also falls under data protection laws. Second, when an individual profile or a group profile (of anonymous data) is applied to an identifiable person, the application of a profile is also subject to data protection law, obliging the controller to process the personal data on a legitimate basis.

If such a purpose includes the transmission of data to third parties, article 11 obliges the third parties – the new controllers – to provide the data subject "*at least the following information, except where he already has it: (a) the identity of the controller and of his representative; (b) the purposes of the processing; (c) any further information such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.*" It might be that the health insurance company asked permission of the data subject to collect all possible data on his health situation from different sources. In this case, the user should be informed about this fact and what is going to happen with this data, e.g., for what purpose the third party collected those data.

The service providers will also collect sensitive data. Article 8 of the Data Protection Directive defines sensitive data as "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*". As already seen above, the processing of such sensitive data is in principle prohibited. Paragraphs 2 and 3 of Article 8 of the Data Protection Directive do nevertheless allow the processing of sensitive personal data when: "*(a) the data subject has given his explicit consent to the processing of those data; or (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in*

connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or (e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims." The Member States can add extra exemptions to the general prohibition.

On the basis of the information the insurance company receives, they automatically decide to raise the premium. But even if the personal data have been lawfully acquired, article 15 grants every person the right "*not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.*" There is an exception: "*(a) person may be subjected to such a decision if that decision is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view.*"

On the basis of the information collected, the MEP receives personalised messages. Although some might be useful, the data subject should have the possibility to refuse these personalised messages. This right can be found in article 14B of the Data Protection Directive: "*The data subject has a right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.*"

We also refer to the problems regarding the opt-in rule (article 13 of the Directive 2002/58) that exist and may arise in the future provides for a right to object (section 6.1.9.). Article 13 further stipulates: "*Where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.*" The opt-out mechanism provided in this paragraph has several disadvantages. The data subject has to declare specifically that he does not want to receive these messages, which puts a burden on him. He might not know who sends the information and he might have to opt out from a number of personalised message systems.

When he opts out, he also loses important information and services. This limits his freedom to opt out to a great extent. People are even considered suspicious when they decide not to use certain services.

Article 6 of the E-commerce Directive 2000/31 obliges the provider of commercial communications, even when they are solicited, "*to ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions: (a) the commercial communication shall be clearly identifiable as such; (b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable; (c) promotional offers, such as discounts, premiums and gifts shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously; (d) promotional competitions or games shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously*." Providing this information should allow users to understand the aim of the messages they receive. It will allow them to distinguish useful from manipulated information. Article 7 of this directive sets out additional conditions for unwanted commercial communications.

Conclusion A lot of information is profiled and transferred to third parties. The persons who collect, process and/or receive the personal data should guarantee that the rules will be respected. The current solutions seem not to provide a proper balance between the risk arising from profiling, the consent for the data collection and workability of the system (giving consent each time is probably not feasible). The obligation of the provider to act in accordance with principle of proportionality may be relevant to resolve the issue. Similarly, the right of the data subject to refuse personal message is, in fact, limited by putting on him the burden of un-subscription and the risk of losing the information or service in which he may be interested.

6.4.2 Service refusal and incomplete personal profiles

Situation description Person is refused a hotel room on the basis of an inadequate profile check, and suffers damage in consequence.

Scenario link *"If you present yourself at a hotel reception desk without an advance reservation, the big hotel chains will run a quick profile on you. The problem is that that it takes time to go through the massive amount of data. As a result, an early warning system is set up that already gives suggestions after only 5 percent of the data has been processed*".

Legal field Data protection – Liability

Legal chapter Data Protection Directive 95/46/EC

Discussion

When personal data are collected and processed, Article 6 (a), (c) and (d) of the Directive 95/46/EC provides that the personal data must be processed fairly and lawfully, the personal data must be adequate, relevant, accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. Here the person was refused a room because of the use of incorrect data and the hotel did not respect several of the conditions described above. The data subject suffered damage. It will be difficult, however, to show who made a mistake, how much damage was suffered because of it and to prove the causal link between the damage and the mistake. According to Article 23 of Directive 95/46/EC, any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the controller for the damage suffered. The crucial question is who will be held responsible or liable for the damage caused by the use of incorrect data. The error could be the consequence of the input of incorrect information. Another possibility is that the hotel misused the information and created a bad profile on the basis of correct information. It will be very difficult to determine which service provider made the mistake. The directive 85/347 on liability of the defective products does not provide for any solution in that situation since it is not applicable to services. The refusal of a room by the hotel can be considered as a prohibited automated individual decision in the sense of article 15 of the Data Protection Directive (cf. supra). Creating the bad profiles on the basis of the information, requesting the information for the service to be granted as well as the undertaking the automated decision on the bases of the profiles has to always be examined as against the anti-discrimination rules. Profiles or decision based on inadequate criteria (health data, nationality, income, etc.) may lead to discrimination of the individuals. It is difficult to determine when it is objectively justified to use such data and criteria, and when they are discriminatory. Further limitation of using of the discriminatory criteria in the Information Society Services may be required.

Conclusion

It will be difficult to hold the hotel liable for the incorrect profiling, not only because the profiling error may have been the result of the activity of different providers, but also because the causal link between the error and damage will be difficult to establish. The evidential issues (procedure) as well as the tort rules and prerequisites (as causation) are regulated by national laws. It will be difficult to meet the traditional tort law preconditions in such situations.

However, as the Data Protection Directive put forwards the principle that any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the controller for the damage suffered (supra), it might well be that the traditional tort requirements do not have to be met. A growing

awareness of the importance of data in the Information Society and its risks might lead to a legal framework offering adequate safeguards for victims of wrongful processing in civil law. Future developments and future case law should clarify this.

6.4.3 Digital virus damages public transport system

Situation description	Digital virus causes chaos and damages to transport system.
Scenario link	*"The city's intelligent traffic system went completely mad (…) centre's main server was attacked by a digital virus."*
Legal field	Liability
Legal chapter	Directive 85/347 on liability for defective products
Discussion	Since the creator of the virus might be untraceable, we should wonder whether the providers of the different traffic services protected their system sufficiently against these attacks and if the traffic control systems were sufficiently protected. Problems will arise again when trying to prove which service provider was responsible for which part of the damage. The principles set out in Directive 85/347 could solve part of this problem if it were updated to be applicable to services and software. The person who created the virus committed a number of criminal offences as defined in the Cybercrime Convention. The virus as such could be considered as a device which is especially designed to commit such criminal offences.
Conclusion	The majority of the criminal offences defined in the Cybercrime Convention require proof that the perpetrator had the intent to commit the specific crime. When a virus is created, however, it could be argued that there does not exist a specific aim or intention. That is why in some situations the specific intention should not be a precondition of liability. Even when there was no bad intention, the creator could still be liable for the civil damage caused.

6.4.4 Crowd management and communication

Situation description	Putting PDA devices in concert mode allows organisers to transmit messages in emergencies but also allows (unwanted) commercial messages.
Scenario link	*"Incidents in the past with big crowds led to the development of crowd management strategies supported by AmI technologies (…) crowds and individual movements are monitored continuously (…) so that any*

incidents are noticed immediately. This time however, the system did not function properly." [96]

Legal field E-commerce

Legal chapter Directive 97/7 on consumer protection in respect of distance contracts – E-Commerce Directive 2000/31 Privacy & Electronic Communications Directive 2002/58

Discussion Article 10 of Directive 97/7 provides that the use of distance communication – other than for automated calling machines and faxes – is only allowed where there is no clear objection from the consumer. Apart from the general criticism that this opt-out system is not suitable or appropriate, the user will have difficulty to set his preferences in such a way that he only receives emergency information and not other commercial information transmitted by the concert organiser. If the concert organiser obliges people to set their devices to concert mode for safety reasons, consumers should be able to react when it is used for other purposes. Article 6 of the E-commerce Directive obliges the concert *organiser* to make a clear distinction between practical information and commercial communications and allows the concert visitor to react if the concert mode is used for purposes other than emergency messages. Article 7 of this Directive sets out additional conditions for unwanted commercial communications. Rules on unsolicited electronic communication as set up by the Privacy & Electronic Communications Directive are also of relevance (see situations 6.1.9 and 6.4.1)

Conclusion Existing rules allow and oblige a distinction to be made between practical and commercial information. Even so, doubts may remain about how easy it will be to enforce such a distinction.

6.4.5 Pseudonymous authentication

Situation description Temporary wireless pseudonymous authentication is possible thanks to new technology.

Scenario link *"…people with implants, through their intelligent proxies were able to effortlessly negotiate, check and download the appropriate concert profiles."*

Legal frame Privacy

Legal chapter Article 8 of the ECHR

Discussion People swallow chips which transmit an identity assigned to a person

[96] Upton, Mick, "Casual Rock Concert Events", June 2005. http://www.crowddynamics.com/Main/Concert risks.htm

until the end of the concert. This allows them to stay anonymous and allows the concert organisers to check the behaviour of people at the concert. Thus, there is a balance between privacy and security.

Article 8 of the ECHR protects the personal life of individuals. This protection implies the right to stay anonymous. The concert organiser needs to ensure the safety and security of the individuals participating in the concert. With the chips, people can stay anonymous and the concert organiser maintains the possibility of being able to control the movements and safety of everybody at the concert.

Even when technology seems to offer intelligent solutions for traditional safety vs. privacy problems, the traditional logic of human rights law has to be applied, i.e., the principle of proportionality and necessity. The Luxembourg Court of Justice of the EU has held in case C-223/98 (Adidas AG) that

"*It is apparent from both the abovementioned case-law and Directive 95/46 that protection for the sphere of private activity of natural and legal persons occupies an important place among the legal principles introduced by the Community legal order. However, that protection neither can nor should be absolute. The Court of Justice has held that restrictions may be imposed on fundamental rights 'provided that they in fact correspond to objectives of general public interest and do not constitute, with regard to the objectives pursued, a disproportionate and intolerable interference which infringes upon the very substance of the right protected.*"

This is the same spirit that inspired the authors of Directive 95/46. They did not consider that the right to protection of privacy was absolute, which would mean a general prohibition on selecting and processing personal data. Rather than laying down an absolute prohibition, the directive indicates the need to ensure a balance between the interests involved and having particular regard to the principle of proportionality. The processing of personal data must therefore be carried out with the consent of the person concerned "or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person ..." The processing must also relate to data which are "adequate, relevant and not excessive in relation to the purposes for which they are processed."

Not all concerts create safety problems. The concert organiser will need to ask consent from persons attending a concert.

Conclusion

New technological developments such as those described in the scenario offer possible solutions to the problems of striking a balance between traditional privacy and security. Their use has to be carefully

assessed within the framework of human rights law.

6.5 RELEVANT AND QUOTED LEGISLATION

Council of Europe - European Convention on Human Rights of 10 December 1948

United Nation Convention on the Rights of the Child of 20 November 1989

Treaty establishing European Communities, (consolidated text), OJ C 325, 24.12.2002

Treaty on European Union (consolidated text), OJ C 325, 24.12.2002
Charter of Fundamental Rights of the European Union, OJ C 341, 18.12.2002, p. 1

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 , 23/11/1995 p. 0031 – 0050

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ L 069, 16/03/2005 p. 0067- 0071*

Working Document on the Surveillance of Electronic Communications in the Workplace, adopted on 29 May 2002, 5401/01/EN/Final WP 55
Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *OJ L 095, 21/04/1993 p. 0029 - 0034*

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *OJ L 144 , 04/06/1997 p. 0019 - 00*

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L 178 , 17/07/2000 p. 0001 - 0016*

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products *OJ L 210 , 07/08/1985 p. 0029 - 0033*

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *OJ L 122, 17/05/1991 p. 0042 - 0046*

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ L 077, 27/03/1996 p. 0020 - 0028*

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ L 167 , 22/06/2001 p. 0010 - 0019*

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, *OJ L 204 , 21/07/1998 p. 0037 – 0048, CONSLEG - 98L0034 - 05/08/1998 - 33 P*

Council of Europe - Cybercrime Convention of 23 November 2001

Convention of Rome on the Law applicable to contractual obligations opened for signature in Rome on 19 June 1980 (80/934/EEC), *OJ L 266, 09/10/1980 p. 0001 - 0019*

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *OJ L 012 , 16/01/2001 p. 0001 - 0023*

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) *O Jl L 108 , 24/04/2002 p. 0051 - 0077*

Belgium Collective Labour Agreement no. 81 of 16 June 1998

7 CONCLUSIONS

The dark scenarios in this document aim to highlight potential vulnerabilities and associated threats when AmI applications go wrong or do not work as expected. That is why the scenarios are labelled dark. Their objective is to identify challenges and issues that need to be addressed for a future (benevolent) development and implementation of ambient intelligence. As such, the dark scenarios are intended to alert policy-makers and AmI developers and designers to the need to develop safeguards to minimise the risks that could emerge in this new intelligent environment.

Many detailed messages can be distilled from the varied situations described in the dark scenarios and from their analytical treatment. We trust that readers of the scenarios agree that it is necessary to anticipate the risks associated with AmI. Such awareness would already be an impact of this report that goes far beyond what a synthesis exercise could achieve. Moreover, as mentioned in the outlook section of this chapter, SWAMI will take the vulnerabilities identified in the scenarios and elsewhere to develop proposals for safeguards and policy options. First, however, a broader reflection on the major issues and threats coming out of this report is presented here. Second, the methodological structure used by SWAMI for the scenario exercise is considered with regard to its utility for other scenario exercises.

7.1 DARK SCENARIOS AND KEY SWAMI ISSUES

The key issues in the SWAMI project relate to privacy, security, identity, trust and the digital divide. Loss of control, dependency, exclusion and victimisation have also been considered by the SWAMI partners.

7.1.1 Privacy

The implementation of AmI bears the risk of compromising our privacy. It is important to be aware of the implications of AmI on private life and private data and to take adequate technical, legal, economic and social measures to protect privacy. The scenarios have shown how privacy could be invaded in the AmI future: identity theft, the little brother phenomenon,[97] data laundering, disclosure of personal data, surveillance and risks from personalised profiling. Although privacy and data protection feature as key issues in the legal analysis of the scenarios, we recognise the uncertainties about what will be regarded as a "reasonable expectation of privacy" and how it might be taken into account in an AmI world.

7.1.2 Security

Security is a key challenge for successful AmI implementation. The scenarios depict security issues in different contexts: security imposed for tele-work, biometrics used for

[97] The Orwellian vision of "big brother" was that the state had the power and technology to engage in surveillance, but with decreasing size and price, surveillance technologies have become "democratised". Today, new threats come from the little brothers, companies, neighbours, even relatives. See Rheingold, H., 2003.

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. Security is critical in the AmI environment. Liability, criminal law and e-commerce are considered in our legal analysis and the possible impacts that arise when there is a lack of security or unsuitable security measures.

7.1.3 Identity

Identity, identification, authentication and preferences play important roles in determining the feasibility of the AmI environment. The scenarios expose and detail these different facets of identity and the consequences when identity-based data are misused, erroneously used or incompletely processed. The legal analysis considers data protection and liability in the context of identity-related issues.

7.1.4 Trust

Sociological studies have shown that in traditional interactions trust is a by-product of informal personal exchanges, but ambient intelligence has the potential to make many of these exchanges obsolete though automation, computer-mediated communication and device-device communication. Thus, conducting more interactions remotely or with computers rather than with humans tends to deprive the users of opportunities for trust building.[98] The human-computer interaction community has recognised the need for building mechanisms for trust and credibility into technology-mediated interaction.[99]

The notion of trust has technical aspects as well as social, cultural and legal aspects. In the scenarios, trust is raised in different connections: trust and confidence, lack of trust (from loss of control, unwillingness to provide some data, contextual misunderstandings), and honesty.

7.1.5 Loss of control

Loss of control is one of the main issues in the SWAMI dark scenarios and 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. It can also emerge when the complexity level of AmI devices or services is too high and consequently does not enable users to get what they want. Strategies should be defined in order to compensate for the complexity and to weaken this feeling of loss of control. Loss of control is featured especially in scenarios one and four, and manifests itself when the interaction between the user and a technology is not in harmony, when the interaction contains weaknesses relating to affordability, transparency and ease of use.

7.1.6 Dependency

Merely by using a technology, the user may become dependent on it, especially when the technology provides benefits and alternative solutions are (no longer) available. The scenarios introduce this topic and highlight social impacts. Several situations are described, such as dependence on personalised filtering, on seamless and ubiquitous communications, on AmI systems (e.g., health monitoring and traffic management

[98] Giddens, A., 1990.
[99] Grabner-Kräuter, S.; Kaluscha, E. A., 2003.

systems) and users' feeling of dependence and frustration when the technology does not work as expected.

7.1.7 Exclusion

The risk of exclusion (vs. inclusion) is raised several times in the scenarios. AmI can give rise to two types of exclusion, voluntary and non-voluntary exclusion. Exclusion can be voluntary, for instance, when a user switches off in order to be left alone or for other purposes. Even with the case of voluntary exclusion, society needs to consider equal rights and opportunities for all, that is making sure that people that switch-off are not deprived of important services.

Unfortunately however, exclusion occurs usually outside people's own will. Related to AmI, exclusion can be the result of lack of interoperability, denial of service, inadequate profiling and data mismatches. This type of exclusion can put individuals to great inconvenience such as non-access to transport, employment. The legal analysis discusses exclusion in the context of interoperability, data protection, liability and conditional access services.

7.1.8 Victimisation

Citizens have a democratic right not to be treated as criminals (unless they are criminals, of course), otherwise, they will be unfairly victimised. Scenarios one and four illustrate victimisation as an AmI impact by describing a disproportionate reaction based on unfounded suspicions. These scenarios also highlight the difficulty in being able to act anonymously (anonymity is regarded as suspicious behaviour) and without being subject to anonymity profiling. The legal analysis considers victimisation in the context of privacy and data protection issues.

7.2 DARK SCENARIOS AND THREATS

In addition to those identified in the dark scenarios, still more concrete threats can be identified, and this will be an objective of future SWAMI work, but some of the major threats are come from surveillance, identity theft, malicious attacks, digital divide and spamming.

7.2.1 Surveillance

Many AmI services depend on acquisition of personal data and their re-use for different purposes. Every citizen/ consumer leaves electronic traces as the price of participation in the ambient intelligence society. These traces make possible new and more comprehensive surveillance of our physical movements, use of electronic services and communication behaviour. These traces will make it possible to construct very sophisticated personal profiles and activity patterns.[100]

The justification for installing surveillance systems typically relates to safety and

[100] For a general discussion, see Marx, G. T., 1995.

security, to countering terrorism and crime. Some scenarios dealt with these topics, notably scenario three where employees are constantly monitored. Surveillance raises privacy and data protection issues, as explained in the legal analysis. One can rightly assume that there is a clear need to delineate and define the boundaries between the private and public spheres. In theory and in the practice of law, this delineation makes it possible to determine when the private sphere has been violated and when the corresponding protection of privacy laws can be applied. In reality, however, the boundaries between the private and public spheres are blurring, a trend that will accelerate as AmI technologies pervade our society. Hence, many existing laws may not adequately address the new realities (they may suffer from lacunae). At the same time, social attitudes towards privacy are in a state of flux (and may always be while any modicum of privacy remains intact). For example, many (most) people are willing to trade off some of their privacy for better security, even if privacy and security are not (necessarily) at opposite ends of a see-saw. Even if surveillance cameras and other surveillance technologies encroach upon our privacy, we are willing to tolerate them if they help to catch criminals and terrorists. (Even so, people recognise the risk of abuses, where innocent people are deprived of their civil liberties.)

7.2.2 Identity theft

Without suitable security, the AmI environment may give malicious persons many opportunities to steal identity information and to use it for criminal purposes. This was also shown in SWAMI Deliverable D1. The threat and risk of identity theft feature in the SWAMI dark scenarios too, especially in scenarios one and three. In addition, a new kind of crime is raised – data laundering – which is detailed in the legal analysis in the context of data protection.

7.2.3 Malicious attacks

Generally, every new technology is plagued by weaknesses (known and/or unknown). Such weaknesses threaten to serve as the backdoor for malicious attackers. Scenarios two and four introduce different aspects of this threat and its possible impacts. The legal analysis mainly refers to liability and criminal law in order to tackle this threat.

7.2.4 Digital divide

Because of its user friendliness and intuitive aspects, AmI technology has the potential to bridge some current gaps in the digital divide but this same technology could also widen the digital divide in regard to unequal access and use. The digital divide is a key issue in one scene in scenario four and features in scenario three.

Scenario two highlights this threat in terms of social and organisational aspects. It shows that ambient intelligence services are not automatically becoming public utilities at the service and benefit of all. In fact, the big investments needed for installation of an ambient intelligence infrastructure may result in an economic rationale for premium services for premium fees, which could exclude those social groups that could benefit most from such services. It is not self-evident that AmI services will become as widespread as mobile communications, especially in developing countries. Apart from these issues, the digital divide has a technological aspect since AmI services have to be intuitive and easy to use.

7.2.5 Spamming

The risk of 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 referenced in scenarios one, two and three. A special focus on profiling is given in scenario four. The legal analysis examines spamming in the context of privacy, data protection and e-commerce.

7.3 THE SWAMI SCENARIO METHODOLOGICAL FRAMEWORK

The SWAMI dark scenarios are not different from other scenario exercises except for their focus on dark situations, on the possible vulnerabilities and weaknesses of future AmI systems, in order to focus on the need to develop safeguards and protections. As a result, we view the SWAMI dark scenarios as a constructive undertaking towards realising a safe and secure AmI.

SWAMI has developed four dark scenarios that encompass both individual and societal concerns, on the one hand, and private and public concerns, on the other hand. These two scenario axis (individual-societal and private-public) have helped us to reduce the virtually infinite number of possible futures that could be developed to a manageable number of four that cut across the everyday life of many people, be it at home, at work, on the road, while travelling or going to public events, and while caring for the environment and for other people and nations.

The methodology used for developing the SWAMI dark scenarios is in line with mainstream scenario exercises, i.e., a combination of desk research and interactive workshops. In addition to the SWAMI scenario stories or scripts, the SWAMI scenarios contain an analytical framework that 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*.

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.

7.4 OUTLOOK

The scenarios and analyses presented in this report are an intermediate step in the

development of safeguards for a world of ambient intelligence. In our subsequent work, SWAMI will specify the vulnerabilities discussed and validated in the light of the interest of various AmI constituencies. The identified opportunities and risks will be contrasted and balanced for each of the affected user groups and applications.

In the next stage of our work plan, we will consider how and to what extent it is possible to overcome the problematic implications of the dark side of ambient intelligence through the use of various safeguards and privacy-enhancing mechanisms (PEMs), the aim of which is to ensure user control and enforceability of policy in an accessible manner and the protection of rights for all citizens in all their roles (private and professional) in the Information Society.

These suggestions will not be made from a merely technical, but rather from a policy, regulatory, functional, practicality perspective since effective privacy enhancing mechanisms have to consist of an appropriate mixture of technical, social and organisational measures that include

- incentives for individuals and organisations to adopt privacy-enhancing technologies, including economic, social and policy incentives,
- contextual factors whereby privacy is balanced against other factors which include: (i) information desires of other actors (employers, marketers, law enforcement), power difference between actors, and (ii) environmental factors such as safety, security and usability. Balance in this context includes examining trade-offs or conflicting interests (e.g., erosion of privacy vs. need to prevent or contain terrorism).
- trust factors whereby information-sharing (and information-hiding) is shaped by trust relationships between actors. Privacy techniques must be responsive to those relationships. Moreover the trustworthiness of ubiquitous computing systems is important, especially in cases where user agents (systems working on users' behalf) are involved.

In order to deal with possible impacts and to implement safeguards and privacy enhancing mechanisms, SWAMI will consider various societal and policy options. These will indicate where responsibilities lie or should lie (and why) as well as aspects of digital behaviour relating to deployment and use of the new technologies. This analysis will also indicate where there are difficulties in regard to the various options, including, for example, the costs involved, attitude and willingness of industry, awareness of consumers, proliferation of standards, and interoperability.

8 REFERENCES

Aarts, E., Harwig R. & Schuurmans, M., "Ambient Intelligence", in P. Denning, ed., *The invisible future. The seamless integration of technology in everyday life*, New York: McGraw-Hill, pp.235-250, 2002.

Alahuhta, P., Jurvansuu, M., Pentikäinen, H., "Roadmap for network technologies and service", *Tekes Technology Review* 162/2004, Helsinki: Tekes, 2004.

Biever, C., "RFID chips watch Grandma brush teeth", NewScientist.com news service, 17 March 2004.

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, A.W., *Guide to Biometrics*, New York: Springer, 2004.

Cabrera, M. & Rodríguez, C., "The role of Ambient Intelligence in the Social Integration of the Elderly" in G. Riva, F. Vatalaro et al. (eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction*, Studies in New Technologies and Practices in Communication, 6, IOS Press, Amsterdam, pp. 265-280, 2005.

COM(2005) 229 final, "i2010 – A European Information Society for growth and employment", Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 1.6.2005.

Daugman, J., "Iris Recognition: Anti-spoofing Liveness Testing, Stable Biometric Keys, and Further Research Directions", presentation at BioSecure project 1st Residential Workshop, Paris, August 2005.

De Hert, P. "Biometrics: legal issues and implications", Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission, January 2005.

Dey, A., Mankoff, J., "Designing Mediation for Context-Aware Applications", *ACM Transactions on Computer-Human Interaction*, Special issue on Sensing-Based Interactions. 12(80), Issue 1, pp.53-80, March 2005.

European Commission, "Information Society Technologies. A thematic priority for Research and Development under the Specific Programme 'Integrating and strengthening the European Research Area' in the Community Sixth Framework Programme, IST Priority, WP 2003-2004", EC, Luxembourg, 2002. http://www.cordis.lu/ist

Friedewald, M., Vildjiounaite, E. & Wright, D., eds., "The brave new world of ambient intelligence: A state-of-the-art review", SWAMI Deliverable D1, A report of the SWAMI consortium to the European Commission under contract 006507, October 2005. http://swami.jrc.es

FTC, "Future Threats and Crimes in an Ambient Intelligent Everyday Environment"

supplied by Qinetiq and Transcrime for IPTS/JRC under contract 22152-2004-06-F7SC SEV GB, July 2005.

Fujawa, J. M., "Privacy Made Public: Will National Security Be the End of Individualism?", *Computers and Society*, 35, Nr. 2, 2005.

Garate, A., Lucas, I., Herrasti, N., Lopez, A., "Ambient Intelligence Technologies for Home Automation and Entertainment", in EUSAI 2004, Workshop "Ambient Intelligence Technologies for Well-Being at Home", 2004.

Gavigan, J.P., Scapolo, F., Keenan, m., Miles, I., Farhi, f., Lecoq, d., Capriati, m., Di Bartolomeo, t. eds., "A practical guide to Regional Foresight", IPTS, Sevilla, EUR 20128 EN, December 2001.

Gettelman, A., "The Information Divide in the Climate Sciences", National Center for Atmospheric research, May 2003.

Giddens, A., *The consequences of modernity*, Cambridge: Polity Press, 1990.

Godet, M., "The art of scenario and strategic planning: tools and pitfalls", *Technological Forecasting and Social Change*, 65, pp.3-22, 2000.

Grabner-Kräuter, S., Kaluscha, E. A., "Empirical research in on-line trust: a review and critical assessment", *International Journal of Human-Computer Studies*, 58, No. 6, pp. 783-812, 2003.

T. Healy, J., Donnelly, B., O'Neill, K., Delaney, K., Dwane, J., Barton, J., Alderman, A., Mathewson, A., "Innovative Packaging Techniques for Wearable Applications using Flexible Silicon Fibres", IEEE 54th Electronic Components and Technology Conference, IEEE, EIA, CPMT, June 2004.

FIDIS, "Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence", eds. Schreurs, W., Hildebrandt, M., Gasson, M., Warwick, K., Fidis Deliverable 7.3., European Commission FP6 funded NoE, August 2005.

Jain, A., Ross, A., "Multibiometric Systems", *Communications of the ACM*, Special Issue on Multimodal Interfaces , Vol. 47, No. 1, pp. 34-40, January 2004.

ISTAG, "Scenarios for Ambient Intelligence in 2010", Edited by Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J. & Burgelman, J.-C., IPTS-ISTAG, EC: Luxembourg, 2001. www.cordis.lu/ist/istag

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. & Rogers, S., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors", National Threat Assessment Center United States Secret Service & Carnegie Mellon University, Washington & Pittsburgh, PA, May 2005.

Knospe, H., Pohl, H., "RFID Security", in Elsevier 2004.
http://www.inf.fh-bonn-rhein-sieg.de

Korhonen, I., Aavilainen, P. and Särelä, A., "Application of ubiquitous computing technologies for support of independent living of the elderly in real life settings" in UbiHealth 2003: The 2nd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Seattle, 8 October 2003.

Krim, J., "Consumers Not Told Of Security Breaches, Data Brokers Admit", *The Washington Post*, 14 April 2005.

Lucky, R., "Connections", Bi-monthly column in *IEEE Spectrum*, March 1999. http://www.argreenhouse.com/papers/rlucky/spectrum/connect.shtml

Maghiros, I., Punie, Y., Delaitre, S. et al., "Biometrics at the Frontiers: Assessing the Impact on Society", Technical Report EUR 21585 EN, Institute for Prospective Technological Studies (IPTS), Seville, 2005.

Marx, G. T., "The Engineering of Social Control: The Search for the Silver Bullet", In: Hagan, J.; Peterson, R. D. (Eds.): *Crime and Inequality*, Stanford: Stanford University Press, pp. 225-235, 1995.

Masthoff, J., "Modelling a group of TV viewers", In: Proceedings of the Future TV: Adaptive instruction in your living room workshop, 2002. A workshop for ITS 2002, onostia/San Sebastian, Spain , June 2, 2002.
http://www.csd.abdn.ac.uk/~jmasthof/FutureTV02paper.pdf

Massini, E.H. & Vasquez, J.M., "Scenarios as seen from a human and social perspective", *Technological Forecasting and Social Change*, 65, pp.49-66, 2000.

Michahelles, F., Matter, P., Schmidt, A., Schiele, B., cApplying Wearable Sensors to Avalanche Rescue: First Experiences with a Novel Avalanche Beacon", *Computer & Graphics*, Vol. 27, No. 6, pp. 839-847, 2003.

Miles, I., Keenan, M, & Kaivo-Oja, J., "Handbook of Knowledge Society Foresight", European Foundation for the Improvement of Living and Working Conditions, Dublin, 2003. This handbook is available in electronic format only: www.eurofound.eu.int.

Müller, B., "Equity in Climate Change – The Great Divide", Executive summary, Oxford Institute for Energy Studies with the support of Shell Foundation, ISBN 1901 795 233, 2002.

Nouwt, S., de Vries, B., & Prins, C., eds., *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, Asser Press, the Netherlands, 2005.

O'Brien, K., Ligtvoet, A., Rathmell, A. and MacKenzie, D., "Using scenarios to support critical infrastructure analysis and Assessment", Deliverable D3.4, Work Package 3, Version 2.0, 15 January 2003, p. 18. Project funded by the European Commission under the "Information Society Technology" Programme.

O'Harrow, Robert, *No Place to Hide*, Simon & Schuster, New York, 2005.

Paciga, M. & Lutfiyya, H., "Herecast: An open infrastructure for location-based services using WiFi, Wireless And Mobile Computing, Networking And Communications", WiMob'2005, IEEE International Conference, pp.21-28, 2005.

Punie, Y., "The future of Ambient Intelligence in Europe: The need for more Everyday Life", *COMMUNICATIONS & STRATEGIES*, no. 57, 1st quarter 2005, pp.141-165, 2005.

Rheingold, H., Smart mobs: The next social revolution - Transforming cultures and communities in the age of instant access, Cambridge, Mass.: Perseus, 2003.

Safire, W., "Goodbye To Privacy", *The New York Times*, 10 April 2005.

Savidis, A., Lalis, S., Karypidis, A. et al., "Report on Key Reference Scenarios", 2WEAR Deliverable D1, Foundation for Research and Technology Hellas, Institute of Computer Science, Heraklion, 2001.

Solove, Daniel J., *The Digital Person*, New York University Press, New York, 2004.

Schneier, B., "Customers, Passwords, and Web Sites", *IEEE Security and Privacy*, July/ August 2004.

Schneier, B., "An easy path for terrorists", 2004. http://www.schneier.com/essay-051.html

Schneier, B., "The Future of Surveillance", *Crypto-Gram Newsletter*, 15 October 2003.

Schneier, B., *Secrets & Lies*, John Wiley & Sons, New York, 2000.

Wilkinson, L., "How to Build Scenarios", *Wired* 3, Special Issue. http://www.wired.com/wired/scenarios/build.html

Zeller, T. "Black Market in Stolen Credit Card Data Thrives on Internet", *The New York Times*, 21 June 2005.

Zeller, T., "For Victims, Repairing ID Theft Can Be Grueling", *The New York Times*, 1 Oct 2005.