Safeguards in a World of Ambient Intelligence (SWAMI)

Threats, Vulnerabilities and Safeguards in Ambient Intelligence

Deliverable D3

3 July 2006

Editors: Michael Friedewald, Ralf Lindner & David Wright

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

DRAFT: Subject to EC approval

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: Friedewald, M., R. Lindner & D. Wright (eds.), *Policy Options to Counteract Threats and Vulnerabilities in Ambient Intelligence*, SWAMI Deliverable D3: A report of the SWAMI consortium to the European Commission under contract 006507, June 2006. http://swami.jrc.es

Contents

1 INTRODUCTION

1.1 CONTEXT

Ambient Intelligence (AmI) describes a vision of the future Information Society as the convergence of ubiquitous computing, ubiquitous communication and interfaces adapting to the user. In this vision, the emphasis is on greater user-friendliness, more efficient services support, user empowerment and support for human interactions. People are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects and an environment that is capable of recognising and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way.[1]

While most stakeholders paint the promise of 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. Taken together, these developments will create a profoundly different information landscape from the one with which we are familiar today and that will have to cope with the following key characteristics:[2]

- Complexity – as hardware capabilities improve and costs reduce, there is continuing pressure to attempt to build systems of ever greater scope and functional sophistication;
- Boundary-less nature of the systems and interconnectedness – few systems have a clear-cut boundary. They are subdivided into systems within systems;
- Unpredictability – all nodes, connected through a common infrastructure are potentially accessible from anywhere at any time, which may result in unpredictable emergent behaviours;
- Heterogeneity and blurring of the human/device boundary as, for example, wearable and/or implantable devices become more widely available and drop in cost;
- Incremental development and deployment – systems are never finished, new features (and sources of system faults and vulnerabilities) are added at a continuous pace;
- Self-configuration and adaptation – systems are expected to be able to respond to the changing circumstances of the ambient where they are embedded.

The scale, complexity and ever-expanding scope of human activity within this new ecosystem present enormous technical challenges for privacy, identity and security – mainly because of the enormous amount of behavioural, personal and even biological data (such as DNA, fingerprints, facial recognition) being recorded and disseminated. Moreover, many more activities in daily life, at work and in other environments, will

[1] IST Advisory Group, K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten and J.-C. Burgelman, "Scenarios for Ambient Intelligence in 2010", Institute for Prospective Technological Studies (IPTS), EC-JRC, Sevilla, 2001; Punie, Y., "The Future of Ambient Intelligence in Europe: The Need for More Everyday Life" in R. Silverstone (ed.), *Media, Technology and Everyday Life in Europe: From Information to Communication*, Ashgate, Aldershot, 2005, pp. 159-80.

[2] Riguidel, M., and F. Martinelli, "Beyond the Horizon - Thematic Group 3: Security, Dependability and Trust", Report for Public Consultation, 2006. http://www.beyond-the-horizon.net.

depend on the availability of AmI devices and services. Questions of ownership and governance of infrastructures and services will thus loom large. The growing autonomy and intelligence of devices and applications will have implications for product liability, security and service definition. There will also be new and massive economic activity in the trading of those techniques that make things smart. One can expect vigorous discussions of who has rights over what information and for what purpose. Finally, there will be a constant struggle to defend this world of ambient intelligence against attacks from viruses, spam, fraud, masquerade, cyber terrorism and so forth. The risk of new vulnerabilities may prove to be one of the biggest brakes on the deployment and adoption of new capabilities and needs to be mitigated.[3] 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.[4]
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.[5]
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.

1.2 CHALLENGES FROM AMBIENT INTELLIGENCE FOR EU POLICY-MAKING

The definition of and provision for safeguards can be seen as critical for the rapid deployment and further development of ambient intelligence in Europe. Moreover, they are in line with those of the IST priority and the broader objectives of the Sixth and forthcoming Seventh Framework Programmes as well as related objectives stated by the Commission, the Council and others. The Framework Programmes emphasise the importance of taking the human dimension into account in ambient intelligence. In doing so, it echoes the *e*Europe 2005 and the i2010 Action Plans that say that Europe should have a secure information infrastructure. To that end, they identify priorities for FP6 and FP7 as including trustworthy network and information infrastructures with an emphasis on emerging technologies such as ambient intelligence. Research activities are expected to

[3] Sharpe, B., S. Zaba and M. Ince, "Foresight Cyber Trust and Crime Prevention Project. Technology Forward Look: User Guide", Office of Science & Technology, London, 2004.

[4] For results see: Friedewald, M., E. Vildjiounaite, D. Wright, I. Maghiros, M. Verlinden, P. Alahuhta, S. Delaitre, S. Gutwirth, W. Schreurs and Y. Punie, *The Brave New World of Ambient Intelligence: A State-of-the-Art Review*, SWAMI Deliverable D1, July 2005. http://swami.jrc.es

[5] For results see Punie, Y., S. Delaitre, I. Maghiros and D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission, November 2005. http://swami.jrc.es.

take into account the human factor in security.[6] The IST 2003 report puts it even more succinctly: "Instead of making people adapt to technology, we have to design technologies for people."[7]

SWAMI aims to formulate and consider how and to what extent it is possible or could be possible in the future to overcome the problematic implications of the dark side of ambient intelligence[8] through the implementation of various safeguards and privacy-enhancing mechanisms, 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 their roles (private and professional) in the Information Society.

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

1.3 STRUCTURE OF THE REPORT

Chapter 2 gives an overview of the five key areas that have been addressed in our analysis of threats and vulnerabilities in a world of ambient intelligence, namely individual privacy, identity, trust, security and the risks of digital divides. These sections discuss the main goals that safeguards seek to achieve, the challenges that ambient intelligence bears for attaining them and the conflict between some goals.

Chapter 3 details the threats and vulnerabilities in each of the areas. Taking into account the four dark scenarios developed in the second SWAMI report, a small number of generic problems are identified that require the formulation of suitable safeguards.

Chapter 4 presents and discusses approaches for technical, socio-economic, legal and regulatory, and cultural safeguards that are considered in order to address one or more of the problems mentioned before.

Chapter 5 concludes the report by presenting recommendations for various groups of stakeholders, ranging from the European Commission and industry to civil society organisations and the individual citizen.

[6] European Commission, "eEurope 2005: An Information Society for All. An Action Plan to Be Presented in View of the Sevilla European Council", COM (2002) 263 final. Brussels, 2002; European Commission. "i2010 – a European Information Society for Growth and Employment", COM (2005) 229 final, Brussels, 2005.

[7] European Commission / Directorate General Information Society, IST 2003: The Opportunities Ahead, Office for Official Publications of the European Communities, Luxembourg, 2003, p. 10.

[8] The dark side of ambient intelligence has been explored in an earlier work package. The results can be found in Punie, Delaitre et al., 2006.

2 KEY POLICY ISSUES

2.1 PRIVACY

In 1890, the US jurists Samuel Warren and Louis Brandeis famously defined privacy as the right to be let alone.[9] If they had lived in today's information age, they might have defined privacy as the right of the individual to decide for himself or herself when and on what terms his or her personal data should be revealed. If they lived in a world of ambient intelligence, any definition of privacy might be a lot more problematic.

Since Warren and Brandeis's time, privacy has been defined and analysed and conjectured about in hundreds, if not thousands, of different ways. In some ways, privacy is like an onion: it has different dimensions or layers.

At least four types of privacy have been distinguished, which relate to personal information, decision-making, bodily integrity and communications.[10] From our own experience, we can distinguish these and one or two other types, as follows:

- There is the privacy of our personal information, for example, of our bank books, medical records, political opinions and moral convictions, but also of much more trivial personal data related to our daily life (name, age, location data, etc.)
- There is the privacy of the physical person, protecting our bodies against disproportional interferences by others and the state. Privacy yields limits to bodily searches, physical constraining, the extraction and use of genetic information (DNA) and biometric data, etc. We wear clothes, not only to keep warm but also to protect ourselves against others inspecting our bodies.
- There is the privacy of our home, a privileged setting where we can relax, let go and be ourselves shielded of from outside interference. We keep doors closed and curtains drawn because there are times when we don't want prying eyes seeing what we are doing, much less for people to come into our homes to have a first-hand look.
- There is the privacy of our thoughts and beliefs. We don't want people looking inside our minds and knowing what we are thinking, let alone steering our thoughts.
- There is the privacy of behaviour. We don't want people to interfere with our social and intimate life, the choices we make, the relations we have and the behaviour we develop. We want our personality, parenthood, friendships, sexuality, leisure and so on, to remain under our control both as regards choice and sharing.
- There is the privacy of our communications. We don't want third parties meddling in our conversations, telephone calls, mail exchanges and electronic interaction. We trust the confidentiality of what are saying to our doctor, solicitor, priest or lover.

---

[9] Warren, Samuel and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. IV, No. 5 [15 Dec 1890]: "The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality."

[10] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?: Authentication Through the Lens of Privacy*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academies Press, Washington, DC, 2003, p. 63. See also Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham - Boulder - New York - Oxford, 2002, pp. 5-20 ("The many faces of privacy").

There is also a strong correlation between privacy and political freedom. We value the privacy of the voting booth, because we don't want people to know how we are marking our ballots. Our privacy is a condition for our full participation in the democratic constitutional state. Hence, privacy has both a negative and a positive function: on the one hand, it works as a shield against interference in individual matters; on the other, it is a precondition for the construction of the public sphere in which democratic political life can take form.[11]

To all of these types of privacy, there are exceptions, because other private or public interests and rights can prevail in the process of balancing competing interests. Moreover, not everyone's sense of privacy is the same: some people are willing to expose their bodies, their homes, their thoughts, their behaviours, sometimes because they value openness and sharing, sometimes for money and sometimes just because they get a thrill from provoking the curious. Hence, privacy is an elusive concept, partly because people tend to draw the line on what they consider to be private at different points on the privacy spectrum.[12]

Thus, the notion of privacy is unstable, complex, difficult to fix. People's perception of privacy is context-dependent, in time and space. Our expectations of privacy may be different according to our age, gender, culture, location, family history, income, educational level and many other factors.[13] And governments' perception of what our privacy should be may be different from ours. It is no surprise that scholars understand privacy in different ways; some argue that autonomy and liberty are the values behind privacy, while others contend it is intimacy, confidentiality or the control over personal information.[14]

We are more likely to expose more of ourselves to our family than to our friends, more to our friends than our work associates, more to our work associates than to third-party businesses, and so on. We are more likely to favour encroachments on the privacy of other people if there are suspicions that those others are criminals or terrorists or if their activities are counter to an equally ill-defined sense of what is in the public interest.

In the Western world, it is often assumed that most people prefer to maintain their privacy rather than giving it away. If they give up some of privacy, they usually want something in exchange – they provide their financial details to their bankers in exchange for a mortgage, their medical background in exchange for hospital services, and educational records in exchange for admission to university. Some people will give away quite a few personal details to their local supermarket for the privilege of having a customer loyalty card, even though such cards are of dubious value. Probably most people don't realise that having such cards simply leave themselves open to spam not only by their supermarket chain but all the other enterprises with which the supermarket chain shares the customer data, even though those practises are bound by the opt-in principle. Many people are willing to forego

[11] De Hert, Paul & Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in Claes, Erik, Anthony Duff & S. Gutwirth (eds.), *Privacy and the criminal law,* Intersentia, Antwerp/Oxford, 2006, pp. 72-76.
[12] Hafner, Katie, "After Subpoenas, Internet Searches Give Some Pause", *The New York Times*, 25 Jan 2006.
[13] See Gutwirth, Serge, *Privacy and the Information Age*, pp. 5-31 ("Privacy's complexities").
[14] See the discussions in Claes, Erik, Anthony Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Intersentia, Antwerp/Oxford, 2006.

some of their privacy to live in a surveillance society because they attach a greater value to their security than their privacy, however they define it.

In some cases, there is a choice, but such individual choices and the negotiability of privacy should be thoroughly questioned because, very often, people are *de facto* obliged to provide (often unnecessary) personal information if they want access to a certain good or service, for example, when they apply for a job, request a bank loan, conclude an insurance contract, rent a flat and so on. In these cases, there is no open market wherein equal actors have the same means, but lopsided balances of power forcing the weak party to give away information. Instead of choice, there is much one-way traffic forcing the weak party to surrender privacy.

In other cases, moreover, we have no choice but to give up some of our privacy because the law has decided so, transcending our choice. For example, by law, we must complete a tax return, we must fill in the census questionnaires, we must (in some countries) possess and carry an ID card (in some countries, such as Belgium, it is an electronic ID card); we must process fingerprints to obtain and use a European passport; if we call or use the Internet, our communication data will be stored for at least six months (during which time, it could be vulnerable to theft or breach of confidentiality and security); and so on.

In still other cases, our privacy may be violated, and we may or may not know that it has been violated. The threats to our privacy, however we define it, can come from many different sources – from prurient neighbours, industry, government, Internet service providers, private detectives and hackers as well as our supposed friends or family.

It's been said that vigilance is the price of freedom. The same can also be said of privacy. If we value our privacy, it behoves us to be aware of the threats to it and to make countermeasures.

In a world of ambient intelligence, the threats to our privacy multiply. In an AmI world, we can expect to be under surveillance ("transparent") wherever we go because the permanent and real-time registration and processing of our presence and behaviour is the precondition – the "code" – of ambient intelligence. The further development of an adaptive and intelligent environment of pervasive and ubiquitous computing is, in fact, dependent on intensive automatic processing of behavioural and thus personal data and, hence, of intensive registration and monitoring. Already, video cameras are mounted almost everywhere in London. It's been said that people in that city are recorded on camera more than 300 times a day.[15] With machine learning and intelligent software, our behaviour and preferences can be predicted. Like our credit cards, RFIDs can be used to monitor what we buy. Networking sensors can monitor what we are doing.[16] Mobile phone companies can monitor where we are. Amazon, Google, the credit card companies know lots about us. And who can slow down the voracious appetite of government to know more about us than all of them put together?

---

[15] See Jordan, Mary, "Electronic Eye Grows Wider in Britain", *The Washington Post*, 7 January 2006: "People in Britain are already monitored by more than 4 million closed-circuit, or CCTV, cameras, making it the most-watched nation in the world, according to Liberty. The group said that a typical London resident is monitored 300 times a day."

[16] "Cybernetic systems that contextualise, learn and act autonomously present fascinating challenges," says the *ARTEMIS Strategic Research Agenda*, First Edition, March 2006, p. 8.
http://www.artemis-office.org/DotNetNuke/PressCorner/tabid/89/Default.aspx

2.2 IDENTITY

The Oxford English Dictionary defines **identity** as the quality or condition of being the same in substance, composition, nature and/or properties. It can be combined with other words with the meaning 'that serves to identify the holder or wearer', as identity bracelet, card, certificate, disc, papers. Our identity is who we are or, at least, how we can be identified.

Identity, which potentially includes attributes as well as personal information, is distinctive to a given individual. For example, when a driver's licence is initially issued, an effort is made to bind the driver's licence number to an identity that is distinct enough to be linked, in theory, to the individual who requested the licence. Part of the identity comprises attributes such as eye and hair colour, height, weight, a photographic image of the individual, and so on.[17]

An **identifier** points to an individual. An identifier could be a name, a serial number, or some other pointer to the entity being identified. Examples of personal identifiers include personal names, social security numbers, credit card numbers and employee identification numbers.

Identities have **attributes**. Examples of attributes include height, eye colour, employer, and organisational role.

Identification is the process of using claimed or observed attributes of an individual to infer who the individual is. Identification can be regarded as a "one-to-many" check against multiple sets of data. **Verification** is the comparison of sets of data to establish the validity of a claimed identity. It is based on a "one-to-one" check.

Authentication is the process of establishing confidence in the truth of some claim. Authentication does not necessarily *prove* that a particular individual is who he or she claims to be; instead, authentication is about obtaining a level of confidence in a claim.

Authorisation is the process of deciding what an individual ought to be allowed to do.

Identity is associated with an individual as a convenient way to characterise that individual to others. The set of information and the identifier (name, label or sign) by which a person is known are also sometimes referred to as that person's "identity". The choice of information may be arbitrary, linked to the purpose of the identity verification (authentication) in any given context, or linked intrinsically to the person, as in the case of biometrics. For example, the information corresponding to an identity may contain facts (such as eye colour, age, address), capabilities (for example, licensed to drive a car), medical history, financial activity and so forth. Generally, not all such information will be

[17] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?: Authentication Through the Lens of Privacy*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academies Press, Washington, DC, 2003, p. 131.

contained in the same identity, allowing a multiplicity of identities, each of which will contain information relevant to the purpose at hand.[18]

2.2.1 Identity and authentication

In applications ranging from electronic commerce to electronic tax filing, to controlling entry to secured office buildings, to ensuring payment, the need to verify identity and authorise access has driven the development of increasingly advanced authentication systems. These systems vary widely in complexity and scope of use: passwords in combination with electronic cookies are used for many electronic commerce applications, smart cards coupled with biometrics allow access to secured areas, and sophisticated public-key mechanisms are used to ensure the integrity of many financial transactions.

While there are many authentication technologies, virtually all of them involve the use of personal information and, in many cases, personally identifiable information, raising numerous privacy concerns. [19]

Authentication can take multiple forms:

- *Individual authentication* is the process of establishing an understood level of confidence that an identifier refers to a specific individual.
- *Identity authentication* is the process of establishing an understood level of confidence that an identifier refers to an identity. The authenticated identity may or may not be linkable to an individual.
- *Attribute authentication* is the process of establishing an understood level of confidence that an attribute applies to a specific individual.[20]

An important difference for AmI is the one between active and passive authentication. Active authentication requires the individual to do something, like showing an ID or putting a finger on a reader. Passive authentication is the preferred authentication method for AmI. Facial recognition systems allow passive authentication that is more convenient for the user; but the impact on privacy and identity is completely different. Passive authentication, for example, does not easily allow the use of PETs or privacy management systems (unless the database system knows what your preferences are) and may be spying on the data subject.

The processes of authentication and identification are related but distinct. While the former may require the verifying party to authenticate an identifier that refers to the individual, the *identification* of an individual is distinct from the authentication of the individual's *claimed* identity. Some authentication technologies (particularly biometric technologies) are used in both processes.[21]

In principle, authentication technologies can both advance and undermine privacy interests.[22]

---

[18] Kent, Stephen T., and Lynette I. Millett (eds.), *IDs--Not That Easy. Questions About Nationwide Identity Systems*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academy Press, Washington, DC, 2002, pp. 18-20.
[19] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, p. 17.
[20] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, p. 10.
[21] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, p. 50.
[22] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?* p. 55.

2.2.2 Identity mechanisms

A variety of identity mechanisms exist. Some of these mechanisms actually identify the person, while others authenticate a person's identity or authorise the person to undertake a transaction or have access to specified data.[23]

Some of these identity mechanisms are based on passive identification, others on active identification.

In AmI, identifying a subject is not the only way to act. Persons can be identified indirectly by their accessories, for example, when objects receive unique identifiers.

1. Cookies identify a computer. Although the user may be anonymous, the cookie identifies the computer and even makes a difference between the different users of the computer. Although the user is not necessarily identified, he becomes 'recognised'.

2. Objects in AmI will receive unique identities. RFID chips will be included in clothes, SIM cards identify mobile phones, GPS systems identify cars, etc. This has a major impact because people might be identified through their objects (their electronic attributes).

3. Our own body and behaviour are the preferred identity mechanisms in AmI. Besides the identification of objects, biometrics is the second important feature of AmI because it uses our body as an identification tool. People can be identified by their veins, fingerprints, iris scans, heart beat, typing behaviour, voice, gait and so on). In theory, this should enhance the comfort of users who don't need to actively identify themselves, thereby reducing ballast (identity papers) and time otherwise consumed by the identification or authentication process.

ID cards / biometric passports

National identity (ID) cards and passports are supposed to identify the person. However, they have had a long history of being forged, which has led to measures such as incorporation of biometrics to make them harder to forge.[24]

The EU has decided that all passport holders, visitors and foreign resident nationals should be fingerprinted.

While passports are more or less accepted by everyone, or at least everyone who wants to travel outside their own country, national ID cards have had a more controversial history. They are accepted by citizens in most EU countries, but not all (UK). Some countries have

[23] In biometrics, verification and authentication stand for confirmation that user A is who he claims to be, that is, verification is one-to-one comparison. Identification means one-to-many comparison: finding who the user is among many people in the database. The user does not necessarily need to claim who is he. Since these processes are closely related to each other, in the rest of this document, the word identification can also mean *for* authentication or verification.

[24] They may be harder to forge, but still not impossible. See, for example, Lettice, John, "Face and fingerprints swiped in Dutch biometric passport crack", *The Register*, 30 January 2006. http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/

imposed a mandatory electronic identity card that can also be used by private companies for identification purposes (e.g., Belgium, see http://eid.belgium.be/).

A British proposal submitted to the EU would see an electronic fingerprint carried on standardised ID cards in Europe. In December 2005, the European Justice and Home Affairs Council approved minimum security standards for national ID cards which some have seen as another step towards a European biometric ID card.

Credit cards, driving licences, national insurance cards

Like national ID cards and passports, credit cards, driving licences and national insurance cards are linked to a particular person, but not quite so strongly. Only the driving licence has a photograph of the individual. Although they have been used to verify the identification of the holder in the past, they are not so widely accepted these days as a substitute for a national ID card or passport (e.g., if you want to hire a car, you need to produce a driving licence *and* a passport / ID card plus a credit card, of course).

Credit card and national insurance numbers don't reveal much information about the individual, even though they are linked to the individual, but some personal data will have been supplied in order to get a credit card or national insurance number.

IP addresses, e-mail addresses and telephone numbers

An individual may be "identified" by her IP address, e-mail address, telephone number, etc. In reality, the "identification" may be limited because none of these addresses or numbers may be closely enough linked with the person to identify the actual person.[25] In other words, they may be akin to a pseudonym or, at best, a partial identity.

Electronic (or digital) signature

The electronic signature directive (1999/93/EC) defines an electronic signature as data in electronic form attached to or logically associated with other electronic data and which serve as a method of authentication. It defines an "advanced electronic signature" as an electronic signature uniquely linked to the signatory and capable of identifying the signatory.

Popular electronic signature standards include the OpenPGP standard supported by PGP and GnuPG, and some of the S/MIME standards (available in Microsoft Outlook). All current cryptographic digital signature schemes require that the recipient have a way to obtain the sender's public key with assurances of some kind that the public key and sender identity belong together, and message integrity measures (also digital signatures) which assure that neither the attestation nor the value of the public key can be surreptitiously changed.[26]

---

[25] An IP address may be assigned to a computer dynamically making it even harder to use it for identification.

[26] Wikipedia, the online encyclopedia, says there is some confusion in the use of the terminologies electronic signature and digital signature: "Electronic signature is often used to mean either a signature imputed to a text via one or more of several electronic means, or cryptographic means to add non-repudiation and message integrity features to a document. Digital signature usually refers specifically to a cryptographic signature, either on a document, or on a lower-level data structure. The confusion in terminology is unsatisfactory in

Computers have enabled us to digitise all sorts of information including that relating to our identity. Hence, a **digital identity** (or electronic identity, **eID**) is the electronic representation of an individual (or organisation). Digital identity mechanisms are not restricted to smart cards. An eID can potentially operate across different platforms, including, for example, mobile phone SIM cards. Whatever media are used, eID schemes need to be able to authenticate users and to support electronic transactions.

As we can be identified in many different ways, so the concept of **multiple identities** has arisen. We may have multiple identities, which serve different purposes in different contexts. Individuals usually have multiple identities – to family, to an employer or school, to neighbours, to friends, to business associates and so on. Thus, different sets of information are associated with an individual in different contexts. Multiple identities might be better termed as a collection of **partial identities**.

Multiple identities (that is, multiple sets of information corresponding to a single individual) may allow individuals to control who has access to what kinds of information about them. The use of multiple identities can be a legitimate strategy for controlling personal privacy in an information society. In addition to providing a measure of privacy protection, the use of multiple identities, even with respect to a single organisation, serves legitimate and desirable functions in societal institutions as well. [27]

To function in the cyber world, people need an identity or multiple identities. In some instances, we can hide behind our cyber identity, that is, to minimise the disclosure of personal information. **Pseudonyms** can be used to mask identity or reveal parts of it for gaining specific benefits such as participation in a loyalty programme, establishing reputation, or proving a legally valid identity in case of dealings with law enforcement. In other instances, this may not be so possible. For example, some service providers, like the government, may require personally identifiable information, so that if we want the service, we must provide the personal data demanded by the service provider.

In some instances, an individual will need to authenticate who he is or will need to authenticate one of his multiple identities. Hence, the individual will need to have some means to choose the appropriate identity to use. In many cases, he will want to avoid linkages. Hence, he will need to be able to access some **identity management system** that will help him to choose the appropriate identity to use in the particular circumstances.

Identity management systems allow users to define different personae for different interaction roles, with the additional benefits of user control of data transfer. The EC-supported GUIDE project regards identity management as involving the maintenance of an individual's complete information set, spanning multiple contexts and transactions and establishing the relationship among various identities with the goal of improving data protection, consistency, accuracy and security in an efficient manner. Two other important EC-funded projects, FIDIS and PRIME, are also concerned with identity management. They are referenced in more detail further on in this report.

---

many respects, and will remain so until usage, especially in statutes and regulations, becomes more standardized." http://en.wikipedia.org/wiki/Electronic_signature

[27] Kent, Stephen T., and Lynette I. Millett (eds.), *IDs--Not That Easy. Questions About Nationwide Identity Systems*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academy Press, Washington, DC, 2002.

2.2.3 Demands for an identity management system

The demands for identity management systems have grown for several reasons:

- Managing multiple identities – The user needs a way to manage his different partial identities.
- Service personalisation (e.g., by mobile operators)
- Combating crime, including terrorism, illegal immigration, fraud
- Online provision of government services – As noted elsewhere, the European Commission and Member States have made determined efforts to provide government services online. Virtually all eGovernment services depend on identity management systems to store authorisation information.

2.2.4 Examples of identity management systems

In today's world, identity management services are offered by so-called Trusted Third Parties, who will verify (**authenticate**) the validity of a particular identity (supposedly) without revealing who is behind that identity.

Early examples of identity management systems are Microsoft's .NET Passport[28] and the DigitalMe system by Novell[29]. While centralised and functionally limited in many respects, Passport associated a unique ID to every user and eliminated the need for remembering multiple IDs and passwords when interacting with online services. The Passport service failed to win wide acceptance because consumers did not like the idea of having Microsoft manage their information.

The multi-industry Liberty Alliance consortium[30] has developed a set of open standards for a so-called federated network identity. The Liberty Alliance standard relies on a decentralised approach, aimed at empowering individual users. Liberty Alliance refers to network identity as the global set of attributes contained in an individual's various accounts with different service providers. These attributes include information such as names, phone numbers, social security numbers, addresses, credit records and payment information. For individuals, network identity is the sum of their financial, medical and personal data, all of which must be carefully protected. For businesses, network identity represents their ability to know their customers and constituents and reach them in ways that bring value to both parties.[31]

Federated identity management systems such as that of Liberty Alliance remove from users the burden of maintaining multiple separate identities on the Web. Such systems allow users to link identity information between accounts without centrally storing personal information. Users can control when and how their accounts and attributes are

[28] http://www.passport.com
[29] http://www.digitalme.com
[30] http://www.projectliberty.com
[31] [GUIDE] Sociological study of IdM issues in Europe: Theoretical underpinnings, v.1, Deliverable 2.1.2.A, 17 December 2004, p. 19.
http://istrg.som.surrey.ac.uk/projects/guide/documents.html

linked and shared between domains and service providers, allowing for greater control over their personal data.[32]

Microsoft has recently announced its own federated identity management system called InfoCard, a virtual ID card and online authentication system. The technology aims to improve online security while reducing complexity for the user and limiting the disclosure of information. The InfoCard system provides the user with several digital identity cards, each of which will hold only the required information, much like a key card that opens a door without knowing who is entering. When visiting a website, the system will automatically find the appropriate InfoCard for that service. Users will no longer need to sign in with a username and password.[33] Microsoft intends to use the InfoCard program in Windows and its forthcoming Internet Explorer 7 browser. InfoCard is part of a broader push by the company to move away from passwords, which Bill Gates has said are "very quickly becoming the weak link" in online systems.[34]

2.2.5 European identity projects

Recognising that the digital representation of identity has all sorts of ramifications, the Commission has provided funding for several identity-related projects (RAPID, GUIDE, FIDIS, etc) aimed at exploring and finding ways of resolving some of these ramifications. (These and other similar projects were referenced in the first SWAMI report.)

In addition to these projects, the Commission launched an eEurope Smart Card (eESC) charter in 1999, bringing together experts from government and industry to address issues of interoperability and security with regard to the deployment of smart cards across Europe. In March 2003, eESC produced an Open Smart Card Infrastructure for Europe (OSCIE), a set of guidelines and technical specifications for the development of smart card technologies.

Building on the OSCIE, in early 2005, the Commission's DG Enterprise launched a new Community programme called IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens), in part to improve collaboration between Member States, a number of which have already introduced their own eID schemes.[35] With participants from the Member States, the IDABC issues recommendations aimed at minimum requirements and common standards for European eID solutions to interoperate. A four-year IDABC work programme was announced in November 2005.

---

[32] [GUIDE] Sociological study of IdM issues in Europe: Theoretical underpinnings, v.1, Deliverable 2.1.2.A, 17, December 2004, p. 19.
http://istrg.som.surrey.ac.uk/projects/guide/documents.html

[33] Sanders, Tom, "Microsoft unfolds next generation authentication", 15 Feb 2006.
http://www.vnunet.com/vnunet/news/2150289/microsoft-unfolds-generation

[34] Bishop, Todd, "Gates tries to win over sceptics on security", *Seattle Post-Intelligencer*, 15 February 2006. http://seattlepi.nwsource.com/business/259522_rsagates15.html. Gates told an RSA security conference that InfoCard would allow consumers to safely manage their identities online. It seeks to provide better security by reducing reliance on usernames and passwords often the target of computer criminals. InfoCard would, said Gates, put the power in the hands of the user. "Microsoft plans virtual information wallet: Gates", Reuters, 14 Feb 2006.

[35] In 1999, Finland became one of the first EU countries to adopt an e-ID card. In Estonia, national e-IDs are mandatory for all citizens and resident foreigners over 15 years of age.

The Commission report in March 2006 that the market for "qualified" electronic signatures (i.e., those with sophisticated technical protection) has grown much more slowly than expected. A number of applications in the pipeline might, however, trigger market growth. These include the use of electronic ID cards for e-signatures. An electronic ID card can be used as an identification document and to provide on-line access to public services by citizens. In most cases, the ID cards will identify the holder and authenticate the signature, as well as enabling the holder to sign.[36]

2.2.6 Identity in an AmI world

In an AmI world, we will need to identify ourselves or to use a partial identity in order to use an AmI service, most probably many times a day. In some instances, the identification or authentication process will be as a result of a conscious, deliberate decision on our part, in which case we may use our eID. In other instances, the identification process may happen automatically, without any intervention on our part.

With intelligence embedded everywhere in an AmI world, our identity may mutate from a collection of our identifiers and attributes or from a partial identity which we create to something that is created by our presence in and movement through that world.[37] Our identity could become an accumulation of not just our attributes and identifiers, as it is today, but an accumulation of where we have been, the services we have used, the things we have done, an accretion of our preferences and behavioural characteristics. Future technologies may pinpoint our identity, without our intervention, through some combination of embedded biometrics that identify us by the way we walk and/or our facial characteristics and/or our manner of speaking and/or how we respond to certain stimuli. Thus, our identities may be determined by our mere presence in the AmI world, whether we agree to being identified or not. Needless to say, this kind of identification process could give rise to a host of security, privacy and trust issues.

Before discussing the threats to identity, we should ask ourselves if the concept of identity itself is under threat. Identity refers to our sense of self and, in that sense, it is not composed only of fixed elements. Our identity in relation to the government might be just a name and an official address, but our identity in our own smaller world is much more complex and of much greater importance (to us). We define ourselves by the clothes we wear (we wear a tie in the office and put on jeans at home), by our facial expressions (we

---

[36] [European Commission], "Electronic signatures: legally recognised but cross-border take-up too slow, says Commission", Press Release, 17 March 2006.
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/325&format=HTML&aged=0&language=EN&guiLanguage=en

[37] Human beings leave a vast amount of processable and thus correlatable electronic traces, generated spontaneously by our presence and movement through the world. New technology enables collection, processing and correlation of this vast amount of data. These evolutions represent more than mere quantitative changes: they induce a significant qualitative shift that can be described by the notions of the 'correlatable human' and/or 'traceable or detectable human'. See Gutwirth S. and P. de Hert, "*Privacy and Data Protection in a Democratic Constitutional State*" in M. Hildebrandt and S. Gutwirth (eds.), *Profiling: Implications for Democracy and Rule of Law*, FIDIS deliverable 7.4, Brussels, 2005, p..26, www.fidis.net. The development of these concepts is the result of networked and interdisciplinary research carried out under the interuniversity research project "The loyalties of knowledge", financed by the Belgian Federal Science Policy Office (see www.imbroglio.be). See also Hildebrandt M., *"Profiling and the Identity of European Citizens"* in M. Hildebrandt and S. Gutwirth (eds.), *Profiling: Implications for Democracy and Rule of Law*, FIDIS deliverable 7.4, Brussels, 2005. p. 42, www.fidis.net

can smile or look into the eyes of another person in a threatening way), by our verbal expressions (the way we talk to the police), our thoughts, behaviour, attitudes and so on.

In short, our identity is very complex and, to a certain extent, we control it.

In an ambient intelligence environment, we are identified through a digital representation of an identity. This digital representation, however, differs from the physical representation we use in the "analogue" world. There is a risk that this digital representation is not very sophisticated, as it may be based on just a few criteria. If I change my physical appearance, the AmI network may not accept my new identity, I may be refused access to certain services because my 'analogue' identity no longer correlates to my digital identity.

Third-party profiling could also compromise our sense of identity in an AmI world too. If our ambient intelligence environment assumes that, based on past activity and preferences, we can be expect to behave in a certain way in the future, we may be presented a course of action which would not have been our first choice. Worse, we may feel obliged to accept the AmI-presented course because it seems what is expected of us.[38] In this way, our sense of identity begins to erode. Such a situation could also be regarded as inimical not only to our personal freedom, but also to democracy itself (this is an instance of the chilling effect which is generally associated with one's recognition that one is under constant surveillance).

2.3 SECURITY

The traditional taxonomy of security threats distinguishes between three main domains in which threats may appear: confidentiality, integrity and availability.[39] Confidentiality implies protection of information from unauthorised use, integrity implies protection of information from unauthorised modification, and availability implies that the system is capable of providing a service when users expect it. The protection properties all rely on the distinction between authorised and unauthorised entities. Protecting confidentiality, integrity and availability is more difficult in a ubiquitous computing environment than in traditional networks for the following reasons:

- *Possible conflict of interests between communicating entities*. In the past, it has been relatively clear who needs to be protected against whom: for example, system owners and operators need to be protected against external attackers and misbehaving internal users; while protecting users against operators was not considered to be a major issue. Nowadays, it is clear that users may need to be protected against operators, and that different parties can have conflicting interests. An example is the typical conflict between the wish for privacy and the interest in service or co-operation. Thus, the concept of multilateral security has emerged. Multilateral security considers the security requirements of different parties and strives to balance these requirements.[40] It also

[38] This AmI phenomenon has been described as cognitive dissonance. See Brey, Philip, "Freedom and privacy in Ambient Intelligence", *Ethics and Information Technology*, Vol. 7, No. 3, 2005, p. 162. "Users may even start experiencing cognitive dissonance, when they believe they want one thing but a smart object tells them they want something else."

[39] Stajano, F., and R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", first Security & Privacy supplement to IEEE Computer, April 2002, pp. 22-26.

[40] Ranneberg, K., "Multilateral Security: A Concept and Examples for Balanced Security", ACM New Security Paradigms Workshop, September 2000, 151-162.

regards all parties as possible attackers and takes into account possible conflicts of interest, negotiating them and enforcing the results of the negotiations.

- *Network convergence* (wireless communication is envisioned to be seamless between different networks of devices, physical objects and smart dust, and between different communication technologies used). This implies that such sensitive operations, such as banking, are frequently performed wirelessly and that during the banking session the user device can switch several times between different wireless networks about which little is known beforehand.[41]
- *Large number of* ad hoc *communications* (communications between nodes which encounter each other more or less unexpectedly). In *ad hoc* communications, it is difficult to distinguish between normal and malicious devices, because little is known beforehand about the nodes in the environment. This implies that it is fairly easy to realise a denial-of-service (DoS) attack (to make the service unavailable) by adding *ad hoc* communicating devices that constantly send messages and ask for replies, thus disturbing normal operations.[42]
- *Small size and autonomous mode of operation of devices*. This makes it fairly easy to steal personal devices and smart dust nodes and to physically attack them (e.g., to destroy or modify the memory).[43]
- *Resource constraints of mobile devices*. Examples are limited battery life (making it easier to arrange DoS attacks by exhausting the battery due to unnecessary communications),[44] processing capabilities (which make it difficult to run sophisticated encryption or pattern recognition algorithms) and limited communication range and broadband.

Moreover, although protecting security in an AmI world is not easy, protection will become more crucial than ever for the following reasons:

- Growing dependency on computer systems (which may become particularly problematic in highly sensitive domains such as traffic management, health care, etc.).
- Growing complexity of computer systems and diversity of versions, along with high competition in the software production market which makes thorough software testing almost impossible: indeed, even with sufficient time available for testing (which is not always the case), it is not easy to predict all possible configurations and interactions between different software components from different providers.
- Increasing number of computers per person and lack of security knowledge of computer users (indeed, extrapolating from past experiences with individual Internet security behaviour, a significant percentage of users will not exercise the appropriate security procedures).
- Lack of user-friendly security mechanisms: neither user authentication, nor configuration of security settings is user friendly. Personal devices are not protected against losses (e.g., users are not reminded to take the device with them). This lack of user friendliness causes users to ignore security rules, to lose personal devices, etc.

---

[41] Stajano, F., and J. Crowcroft, "The Butt of the Iceberg: Hidden Security Problems of Ubiquitous Systems", in Basten et al. (eds.), *Ambient Intelligence: Impact on Embedded System Design*, Kluwer, Dordrecht, 2003.

[42] Creese, S., M. Goldsmith and I. Zakiuddin, "Authentication in Pervasive Computing", First International Conference on Security in Pervasive Computing, Boppard, Germany, 12-14 March 2003, pp. 116-129.

[43] Becher, A., Z. Benenson and M. Dornseif, "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks", Third International Conference on Security in Pervasive Computing, York, UK, April 2006, pp. 104-118.

[44] Stajano, F., and R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", first Security & Privacy supplement to IEEE Computer, April 2002, pp. 22-26.

- Blurring of boundaries between work and personal use of devices. This means that personal use can threaten not only personal data, but also corporate data, and vice versa.
- Growing opportunities to make money via computers. This can include legitimate opportunities like e-commerce, games or mobile services but also cybercrimes including phishing or data laundering. Killing somebody via arranging a denial-of-service attack on the steering wheel of his car over wireless networks is something that an attacker might try simply out of curiosity. The blurring of the boundaries between the real and virtual worlds makes such a murder feel as real as a computer game.

2.4 TRUST

Digital computing technology increasingly comes to provide mediation between human actors and the world. As such, these technologies structure, constrain and enable our engagement with and experience of the world.[45] Simply said, our life is increasingly intertwined with or related to digital technology. In order to put digital technologies to satisfactory use, and in order to have a convenient and useful interaction with and through technology, trust is a fundamental precondition. The often reported lack of trust in e-commerce demonstrates that insufficient trust can lead to users "staying away" from a technology altogether.[46]

Traditionally, the issue of trust in computers is taken to be one of security and the development of safer and more dependable systems. While the technical security approach is not to be discounted, especially in high-risk systems implementations, focusing exclusively on technical solutions to the problem of trust is not adequate in increasingly digitalised environments.

Many studies on trust in computer-mediated communication fall under the notions of online trust – how do we trust in electronic environments and what relevance has trust in computer-mediated communication, not only between sender and receiver, but also between interface and user? Many draw on traditional sociological conceptualisations of trust,[47] but more technical approaches seem to relate trust directly to the construction of secure systems, thereby implying that users are purely rational, economical actors.[48]

A precursor of trust is the assumption of risk. Hazards abound in late-modern society, are fundamentally changing and deepening our need for trust. Had we not trust in much of the apparatus of late modern society, we would not be able to act at all, we would be tied to our bed for fear of venturing out into a society permeated by seemingly inescapable danger. Trust can be conceptualised as "a willingness to enter into interaction under the

[45] Ihde, D., *Technology and the Lifeworld: From Garden to Earth*, Indiana University Press, Bloomington, 1996.
[46] Grabner-Kräuter, S., and E. A. Kaluscha, "Empirical Research in on-Line Trust: A Review and Critical Assessment", *International Journal of Human-Computer Studies*, Vol. 58, no. 6, 2003, pp. 783-812; IST Advisory Group (ISTAG), "Trust, Dependability, Security and Privacy for IST in FP6", Office for Official Publications of the European Communities, Luxembourg, 2002.
[47] Nissenbaum, H., "Securing Trust Online: Wisdom or Oxymoron", *Boston University Law Review*, Vol. 81, no. 3, 2001, pp. 635-64.
[48] See Roussos, G., and T. Moussouri, "Consumer Perceptions of Privacy, Security and Trust in Ubiquitous Commerce", *Personal and Ubiquitous Computing*, Vol. 8, no. 6, 2004, pp. 416 – 29; Riegelsberger, J., M. A. Sasse and J. D. McCarthy, "The Mechanics of Trust: A Framework for Research and Design", *International Journal of Human-Computer Studies*, Vol. 62, no. 3, 2005, pp. 381-422.

face of uncertainty".[49] Trusting, then, is very much an active stance, as opposed to background human phenomena such as confidence or faith. If trust is not reciprocated or turns out to be imprudently given, we regret our action of having extended trust. If confidence results in disappointment, we cannot but ascribe this to bad luck. Trust, then, is an assumption of others' competence or benign nature, while disappointed confidence will be ascribed to external factors, not something intrinsic to an interaction partner, whom we may still trust.[50] Thus, trust has to do with the experience of actors and acting rather than factors. Trust can be strategically managed at a social level, while confidence works as an ambient background premise.

In his theory of trust, Niklas Luhmann stresses the importance of trust for the reduction of experienced risk in complex environments, and the accompanied increase of possibilities for experience and action when we do trust. Trust, in Luhmann's conception, is a feature of a relation that "brackets" external uncertainty and replaces this with an internal experience of certainty, allowing for continued interaction. According to Luhmann, by trusting we accept our own and others' limitations in predicting the future, especially as the future is structured by the freedom of others to act as they see fit. Trust, then, as a reducer of societal complexity is different from security obtained through political, judicial or economical domination. Indeed, trust, and not necessarily objective security, becomes an increasingly important strategy in highly complex societies, where the outcomes of actions are, and are experienced to be, highly contingent and hence highly risky and where the scope for action and interaction is extensive. This also means that trust is no static construct but a highly dynamic process where the premises of trust are constantly monitored and reassessed. This does not only occur on a rational level but also includes weak factors like our attitude towards technological solutions or the subjective perception of the situation (see figure 1). It is hence not enough to implement trustworthy technological solutions; they also have to be embedded in a socially and organisationally trustworthy way.

Further, trust as a strategy for coping with social complexity means a necessary departure from traditional forms of social contracts such as familiarity. Given the speed with which new technologies emerge, pervade into and change our lives, and given the complexity already inherent in technology and social structure, we cannot relegate our engagement with the world to familiarity, as that which is familiar today may be estranged or change its status tomorrow, due to new insights and new knowledge. Late-modern society is one of reflexivity and radical scepticism towards claims of essentialist truths and objectivity.[51]

[49] Luhmann, N., *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*, 4th ed., Lucius & Lucius, Stuttgart, 2000.
[50] Offe, C., "How Can We Trust Our Fellow Citizens?", in M. E. Warren, *Democracy and Trust*, Cambridge University Press, Cambridge, 1999.
[51] Beck, U., A. Giddens and S. Lash, *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*, Stanford University Press, Stanford, 1994.

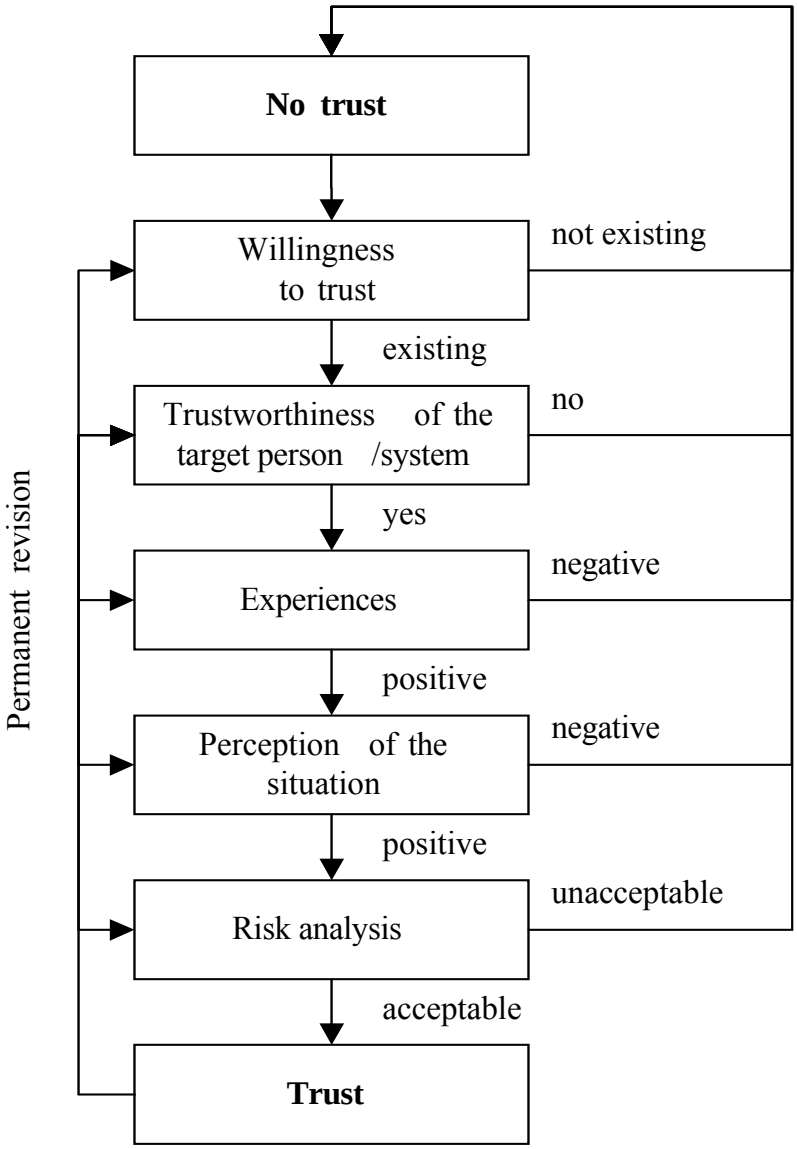

Figure 1: Trust building process

Thus, it is fair to say that the fixation on security is not enough, because trust has its roots in a unique human and cannot, therefore, be grasped with the rational actor assumptions that normally underlie the technological approaches to trust.

In engineering visions of ambient intelligence, technology is invisible in practice, functioning silently in the background – this entails the search for perceptual transparency in interaction – the tool itself should be invisible, non-focal, while the tasks and results are ready-to-hand.[52] This may lead to a conflict between the goals of opacity and transparency/invisibility. As technologies that exist in the background are deliberately designed to be transparent and invisible, they may also bring with them a kind of distrust

[52] Weiser, M., and J. S. Brown, "The Coming Age of Calm Technology", in P. J. Denning and R. M. Metcalfe (eds.), *Beyond Calculation: The Next Fifty Years of Computing*, Copernicus, New York, 1997, pp. 75-85; Aarts, E., R. Harwig and M. Schuurmans, "Ambient Intelligence", in P. Denning, *The Invisible Future: The Seamless Integration of Technology in Everyday Life*, McGraw-Hill, New York, 2002, pp. 235-50; Streitz, N. A., and P. Nixon, "The Disappearing Computer", *Communications of the ACM*, Vol. 48, no. 3, 2005, pp. 32-35.

that, rather than being manifest, is latent and potential. While technological transparency is thought to provide the ideal task-oriented situation, it also effectively black-boxes the overall technological environment, makes it opaque and intangible, complicating trust based on a disclosure of intentions and qualifications in that it hides its presence, and becomes absent – something that is somehow there, but unseen, working tacitly, perhaps unsettlingly, in the background. The intentions and the power relations implemented in the system and the way the system works on more than a mere task level is effectively concealed, and observation, control and empowering of inhabitants are withheld. This leaves no room for a "place" for interaction, no node where action can be taken, and the system, and all that it entails, judged or contemplated. Not only does the background "presence-in-absence" status of such systems raise concerns about privacy and data access ("Who controls the data I give out? Who watches me now?"), but arguably they also complicate the giving out of trust because the object, the other or some index of presence is missing. The direction of trust, then, is free-floating, abstract and distributed, rather than localised, visible and embedded in present situations.

Trust is a necessary feature of life in contemporary societies, as we are surrounded by various kinds of hazards, and as a time-space distance exists between actors and expert systems that manage the risks. We no longer exist in close-knit communities, allowing for deep knowledge, traditions and the visibility of the geographically co-located other.[53] Giddens describes this as a process of disembedding – a continuous uprooting and displacing of social relations from close communities to highly complex, functionally differentiated systems, complicating and challenging trusting relations. The reverse process is, in Giddens' terms, the re-embedding of social relations – similar to national politicians, normally known only through the media, who tour the pedestrian streets, shaking hands and talking casually with voters. Politics, in this way, gains a body, a real voice, a pleasant attitude (even if strategically calculated), and a seeming presence in the immediate, mundane and meaningful surroundings.

2.5 DIGITAL DIVIDE

2.5.1 Framing the term

The term "digital divide" was coined by Lloyd Morrisett, the former president of Markle Foundation, in 1995 to denote the gap, the divide "between those with access to new technologies and those without" [54] or between the information "haves" and "have-nots".

Dimensions

At a first glance, the digital divide concept encompasses two basic dimensions: the **global**, between developing and developed societies and the **social**, which relates to the information haves and have-nots even within the same nation. Norris adds another

[53] Giddens, A., *The Consequences of Modernity*, Polity Press, Cambridge, 1990.
[54] National Telecommunications and Information Administration (NTIA), *Falling through the net: Towards Digital Inclusion. A Report on Americans' Access to Technology Tools*, U.S. Department of Commerce, Economics and Statistics Administration, National Telecommunications and Information Administration, Washington, 2000. http://search.ntia.doc.gov/pdf/fttn00.pdf

dimension, that of **democratic** divide, which signifies the difference between those who do, and do not, use digital resources to engage, mobilise and participate in public life.[55]

Aspects

The digital divide is a multidimensional phenomenon, a varying landscape that manifests itself in a range of indigenous factors and external structures[56]; as such, it is quite difficult to examine all of its facets. In the paragraphs that follow, however, we provide our framing of the term and analyse aspects that have been so far identified and debated internationally in various research studies and other publications. Often these aspects co-exist and interact with each other.

Physical access

Physical access is the quantitative side of the digital divide[57], and is defined basically as the availability of ICT infrastructure. It mainly has to do with the lack of sufficient income to be able to purchase the equipment or to access commercial services or content of use or interest, creating thus a divide between those who are "connected", and those who are "unconnected".[58] In this context, the degree of affordability of the infrastructure is very low, in the sense that many people cannot afford to be connected.

Socio-economic status and income are an important determinant in the issue of Internet access. Generally, the results show that Internet access correlates closely with income.[59] Hoffman and Novak mention that respondents in the United States whose household income is above the average income of $40,000 report higher levels of access, use, home computer ownership and PC access at work and examine race differences within income levels.[60]

Many people think that the problem of digital divide is solved as soon as everyone has a computer and a connection to the Internet.[61] However, researchers have expressed well-founded concerns that physical access is not the sole answer to the issue. Already by the

---

[55] Norris, Pippa, *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge University Press, Cambridge and New York, 2001.

[56] Gourova, Elissaveta, Christoph Hermann, Jos Leijten and Bernard Clements, *The digital divide - A research perspective. A report to the G8 Opportunities Task Force*. Technical Report EUR 19913 EN. DG JRC/IPTS, Seville, 2001. http://fiste.jrc.es/pages/detail.cfm?prs=708

[57] Bolt, David B., and Ray A. K. Crawford, *Digital divide: Computers and our children's future*, TV Books, New York 2000.

[58] Daskala, Barbara, *Networks and Divides: A Digital Divide perspective*, London School of Economics and Political Science, MSc Dissertation, 2001.

[59] National Telecommunications and Information Administration (NTIA), *Falling through the net: Towards Digital Inclusion. A Report on Americans' Access to Technology Tools*, U.S. Department of Commerce, Economics and Statistics Administration, National Telecommunications and Information Administration, Washington, 2000; van Dijk, Jan and Kenneth L. Hacker, "The Digital Divide as a Complex and Dynamic Phenomenon", *The Information Society*, Vol. 19, pp. 315-326, 2003; http://web.nmsu.edu/~comstudy/tis.pdf; Hoffman, Donna L., and Thomas P. Novak, "Bridging the Racial Divide on the Internet", *Science*, Vol. 280, 1998, pp. 390-391; Kruger, Danny, *Access Denied? Preventing Information Exclusion*, Demos, London, 1998.

[60] Hoffman, Donna L, Thomas P. Novak, "Bridging the Racial Divide on the Internet", *Science*, Vol. 280, 1998, pp. 390-391.

[61] van Dijk, Jan, Kenneth L. Hacker, "The Digital Divide as a Complex and Dynamic Phenomenon", *The Information Society*, Vol. 19, 2003, pp. 315-326. http://web.nmsu.edu/~comstudy/tis.pdf

end of the 1990s, the debate started to shift towards the social aspects of the divide, which are now regarded as equally as important as physical access.

Knowledge and skills

Knowledge and skills are the next most important aspect of the problem and one that has come to the fore of the debate.[62] Digital knowledge and skills are not only the skills needed to operate computers and network connections; also needed are the skills to search, select and process information from a superabundance of sources.[63] Even if they have the necessary physical access to ICT infrastructure, many people do not have sufficient digital skills and knowledge that would allow them to take advantage of the full range of benefits offered by the new technologies. There are people who do not have the ability to perform simple tasks with the computers and the Internet.[64] For many disadvantaged groups, access to these skills is still limited. As Kruger observes, simply having access to the equipment is only the beginning of making use of ICT, because people require certain skills to navigate ICT services and to use them effectively.[65] The insufficient user-friendliness of many systems, applications, uses and jargon as well as the often inadequate education or social support often make people feel confused and intimidated by the prospect of using the ICT. This can represent a more significant barrier to ICT enthusiasm than the lack of access to hardware.

Content

Bolt & Crawford define content as the qualitative side of the digital divide.[66] According to a report published by the Children's Partnership, the provision of useful content is deemed as equally important as the physical provision of equipment. Among other things, useful content must include information in multiple languages and opportunities to create content and interact with it so that it is culturally appropriate[67]; but most importantly, information should be adequate to the level of literacy.

In this respect, much of the current content on the Internet is not accessible and/or useful for most potential users. It can be argued that it is easier to access stock market information from around the world than to find out about job opportunities in your local community. In that sense, the content of the Internet is almost exclusively useful or even apprehensible to professionals and academics. People that do not fall in this category, even if they have access to PCs and the Internet, are becoming marginalised, disadvantaged, excluded and underserved. The problem of content is directly connected to that of skills: as people become more confident with ICT, it will become more relevant to them.[68]

---

[62] Morino Institute, *From Access to Outcomes: Raising the aspirations for technology initiatives in low income communities*, Working Paper, Reston, VA, 2001. http://www.morino.org/divides/report.htm.
[63] van Dijk, Jan and Kenneth L. Hacker, "The Digital Divide as a Complex and Dynamic Phenomenon", *The Information Society*, Vol. 19, 2003, pp. 315-326. http://web.nmsu.edu/~comstudy/tis.pdf
[64] Perri 6 and Ben Jupp, *Divided by information? The "digital divide" and the implications of the new meritocracy*, Demos, London, 2001.
[65] Kruger, Danny, *Access Denied? Preventing Information Exclusion*, Demos, London, 1998.
[66] Bolt, David B., and Ray A. K. Crawford, *Digital divide: Computers and our children's future*, TV Books, New York 2000.
[67] Lazarus, Wendy and Francisco Mora, *Online content for low-income and undeserved Americans: The digital divide's new frontier*, The Children's partnership, Santa Monica, 2000.
[68] Kruger, Danny, *Access Denied? Preventing Information Exclusion*, Demos, London, 1998.

Digital red-lining – exclusion by information

The advent of new technologies has enabled companies to collect a vast amount of personalised data from current and prospective customers, through purchasing information and surveys. By using special data matching techniques, companies are able to make investment and marketing decisions by targeting certain groups. This means that all organisations are increasingly able to exclude large numbers of people from access to basic services and opportunities by selecting more or less "valuable" customers. Profiling facilitates control of consumer behaviour as well as the construction of consumer identities; the latter inhibits social mobility and contributes to people's exclusion.[69]

Red-lining[70] has triggered a somewhat reverse concern from the one that has been contemplated until now. Information technology can actually be itself an engine of exclusion and people are not only excluded *from* information but *by* information as well.[71]

Cashless society

The use of electronic money, credit and debit cards is gradually increasing as it has lower administrative costs than traditional cash and it makes transactions easier. However, the concern here lies in the fact that this new form of money is principally used by the better off, who are no longer willing to subsidise the higher costs of the use of traditional cash by the old and poor, who lag behind, able to use only physical money[72]. In some European countries, such as Netherlands and Norway, retailers demand electronic payments or charge more for accepting cash and in Britain the electronic transfer is already a common practice. Plastic money may be more convenient and more suited for transactions in the e-world, but for those who do not have or cannot get or do not want to use a credit card, they are or will be excluded from many electronic services.

Therefore, people will not only need a bank account but also an electronic payment card.[73] Nevertheless, it is likely that the better off will be offered the services first. Participation in the new e-cash- powered economy will require infrastructure and knowledge, which are likely to be more readily available to the better-off than to the poor who cannot afford to buy a computer or pay for Internet services.

Determinants

In addition to the afore-mentioned aspects, many researchers have identified other determinants of the divide, including the following:

---

[69] Kruger, Danny, *Access Denied? Preventing Information Exclusion*, Demos, London, 1998.

[70] The term "red-lining" refers to a system developed in the nineteenth century by drawing colour coded maps of London showing the estimated affluence of the inhabitants in different boroughs and is used to describe the deliberate avoidance of certain large areas by the sellers of insurance (Kruger, 1998). The concept of the 21st century "digital red-lining" is not very far from the 19th century one.

[71] Perri 6 and Ben Jupp, *Divided by information? The "digital divide" and the implications of the new meritocracy*, Demos, London, 2001.

[72] It is estimated that around 20 per cent of the British population does not have access to individual financial packages and between 5 and 8 per cent has no financial support at all, including current accounts (Kruger, 1998). The proportion of poorer people with current accounts is gradually rising, but in the UK nearly 45 per cent of the poorest fifth of the population does not have a current bank account (Perri 6 & Jupp, 2001).

[73] Perri 6 and Ben Jupp, *Divided by information? The "digital divide" and the implications of the new meritocracy*, Demos, London, 2001.

Age – Studies indicate that Internet use is higher among younger groups, i.e., those in the 16-44 age bracket, and that those over 45 are less likely to own a PC and connect to the Internet.[74]

Gender – This determinant regards the gender gap, where men are more likely to go online than women. Although the gender gap appears to have less influence on the digital divide, and is not as high, for example, as that of socio-economic status or education[75], still women are relatively absent from computer science and the design of ICT products[76]. According to EuroBarometer[77], in all European countries, men use the Internet more frequently than women. It is also argued that the gender gap is greatest around the creation of ICT rather than its use.[78]

Race and ethnicity – Race and ethnicity are crucial variables and in some studies are addressed separately. The issue of race in relation to the digital divide has been particularly studied by Hoffman & Novak.[79] In general, groups of different racial and ethnic backgrounds use the Internet to different degrees and Caucasians are most likely to have access to computers and the Internet. According to Bolt & Crawford, the racial digital divide exists at every income level save the very highest.[80]

Education – According to the NTIA report, in both 1998 and 2000, Internet use rose with higher levels of education. People whose highest level of education was a bachelor's degree or higher had the highest Internet use.[81] Also, employed people are more likely to have access to computers and the Internet than the unemployed.[82] Apart from that, the advent of the information age has changed job qualifications, requiring special skills and

---

[74] National Telecommunications and Information Administration (NTIA), *Falling through the net: Towards Digital Inclusion. A Report on Americans' Access to Technology Tools*, U.S. Department of Commerce, Economics and Statistics Administration, National Telecommunications and Information Administration, Washington, 2000; Kruger, Danny, *Access Denied? Preventing Information Exclusion*, Demos, London, 1998; Turow, Joseph, and Lilach Nir, *The Internet and the family 2000: The view from parents, the view from kids*, Annenberg Public Policy Center, University of Pennsylvania, 2000. http://www.asc.upenn.edu/usr/jturow/Adobe%20I&F%202000%20fixed.pdfVenkatesh, Viswanath, and Susan A. Brown, "A longitudinal investigation of personal computers in homes: Adoption determinants and emerging challenges", MIS Quarterly Vol. 21, No. 1, pp. 71-102, 2001.

[75] [EC] *eInclusion revisited: The Local Dimension of the Information Society,* Commission Staff Working Document, Brussels, 2005.
http://ec.europa.eu/employment_social/knowledge_society/docs/eincl_local_en.pdf

[76] Strategies of Inclusion: Gender and the Information Society (SIGIS)
http://www.rcss.ed.ac.uk/sigis/

[77] Eurobarometer, June 2003 (EU-15) /July 2003 (10 New Member States) quoted in "eInclusion revisited: The Local Dimension of the Information Society", Commission Staff Working Document, 2005. See also http://ec.europa.eu/public_opinion/index_en.htm

[78] Faulkner, W., *Women, gender in/and ICT: Evidence and reflections from the UK*, Strategies of Inclusion: Gender in Information Society (SIGIS), Deliverable IST-2000-26329, 2000.

[79] Hoffman, Donna .L, and Thomas P. Novak, "Bridging the Racial Divide on the Internet", *Science* , Vol. 280, pp. 390-391, 1998.

[80] Bolt, David B. and Ray A. K. Crawford, *Digital divide: Computers and our children's future*, TV Books, New York 2000.

[81] National Telecommunications and Information Administration (NTIA), *Falling through the net: Towards Digital Inclusion. A Report on Americans' Access to Technology Tools*, U.S. Department of Commerce, Economics and Statistics Administration, National Telecommunications and Information Administration, Washington, 2000.

[82] Turow, Joseph, Lilach Nir, The Internet and the family 2000: The view from parents, the view from kids. Annenberg Public Policy Center, University of Pennsylvania, 2000.
http://www.asc.upenn.edu/usr/jturow/Adobe%20I&F%202000%20fixed.pdf

thus putting many people who do not possess these skills at a disadvantage: "A pair of strong hands are not what they used to be. Now those hands have to be able to use a keyboard".[83]

2.5.2 Digital divide in a world of ambient intelligence

In the context of our information or digital world, access to ICT has become important and indispensable. Those who do not have access to the new technologies are highly disadvantaged or even excluded. In a world of ambient intelligence where technology is undoubtedly much more pervasive than today, access to and use of it becomes even more important: it will be actually part of our everyday life. In this context, digital divide is a crucial issue for societies and it is important to consider its trend: will AmI technologies contribute to the closing or further widening of the gaps?

In general, it seems that AmI will narrow some gaps while widening existing or creating new ones at the same time. Specifically, in terms of physical access to AmI equipment and infrastructure, this is likely to improve, since AmI applications will form an intrinsic part of our every day lives and at least the basic infrastructure is bound to be forthcoming to the majority of the people. Besides, chances are high that the AmI infrastructure will become cheaper and thus more affordable for larger parts of society (although it could also be argued that the network will be more complex, thus the cost higher for the providers). Furthermore, because of the envisioned user friendliness of AmI technology, the required skills and knowledge for its use will be less than that required today to use mobile phones, personal computers and the Internet, thus enabling more people to use its applications and receive the expected benefits. The majority of people are expected to be at least moderately computer literate, especially given the extent of use of technologies in everyday life.

On the other hand, there will still be a percentage of the population that will not have access to AmI applications and even a greater percentage that will have access only to basic infrastructure and not to more sophisticated equipment, thus excluding them from accessing the full benefits of the AmI environment. Moreover, skills and knowledge remain a limiting factor. In a society with extreme levels of technology pervasiveness, people that do not possess the knowledge or the skills to use AmI to some extent will be more seriously excluded than today. It could be argued that though the divide in terms of knowledge and skills may narrow, the divide wherever it exists would be far more dramatic and serious in nature. In an AmI environment, profiling is a prerequisite for many applications, which will provide more opportunities for companies and other organisations to target specific groups, excluding and discriminating other people, on the basis of their profiles.[84]

---

[83] Bill Radley quoted in Kruger, 1998.

[84] For more detailed information on this particular issue, see section 3.6.2 Exclusion and Discrimination. Also, profiling has been defined in different ways, but we like the explication given by Daniel J. Solove in his book *The Digital Person*: "Profiles work similarly to the way that Amazon.com predicts which products customers will want to buy. They use particular characteristics and patterns of activity to predict how people will behave in the future… As Oscar Gandy observes, the use of profiling to form predictive models of human behavior incorrectly assumes that 'the identity of the individual can be reduced, captured, or represented by measurable characteristics." Profiling is an 'inherently conservative' technology because it 'tends to reproduce and reinforce assessments and decisions made in the past.'" Solove, Daniel J., *The Digital Person*, New York University Press, New York, 2004, p. 181. Solove cites Gandy, Oscar H. Jr., "Exploring Identity and Identification in Cyberspace", *14 Notre Dame J.L. Ethics & Public Policy* 1085, 1100 (2000). Closer to home, the EC-funded FIDIS project says "Profiling activity consists of extracting

Apart from that, serious concerns exist about the persistence of digital divides with regard to income, education and specific age groups[85], as well as gender and race / ethnicity. Should no measures be taken towards closing these divides, they will continue to exist more or less to the same degree as degree as today. The gender gap should, however, be less pronounced than it is today, assuming that more women become confident enough to use new technologies.

The global dimension of the digital divide between developed and developing countries is likely to remain the same or even grow. As long as the gap between developing and developed nations in general does not close, the digital divide will also widen, especially as new technologies emerge, which the under-developed societies do not have access to or cannot use. In effect, certain regions will most likely face the problem of accumulated digital divides.

useful information from a current context related to the user, identifying the users' needs and selecting suitable services in order to enable that the smart home behaves according to the users' preferences, actions and expectations." Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS Deliverable D7.3, Brussels, 2005, p. 9. www.fidis.net Thus, in both "definitions", there is a sense of compiling a profile of an individual based on previous activity. Profiling in this sense is instrumental in the personalisation of services, i.e., based on past activity, Amazon (and others) assume that the "customer" might be interested in buying some other similar or related items. Government profiling could be regarded in a somewhat different light, however. The US government's ill-starred Total Information Awareness (TIA) and Computer-Assisted Passenger Pre-Screening System (CAPPS II) programs assumed, for example, terrorists' characteristics could be reduced to a template which could be used to search for others who matched the template. This is the way in which Robert O'Harrow uses the term: "Using artificial intelligence software and insights from profiling programs he'd [the reference is to Hank Asher, the owner of Seisint Inc.] created for marketers over the years, he told Seisint's computers to look for people in America who had certain characteristics that he thought might suggest ties to terrorists." O'Harrow Jr, Robert, *No Place To Hide, Free Press, New York, 2005*, p. 99. Security expert Bruce Schneier uses the term in this latter sense too. "To profile is to generalize. It's taking characteristics of a population and applying them to an individual." Schneier, Bruce, *Beyond Fear*, Copernicus Books, New York, 2003, p. 134. It should come as no surprise, then, that profiling is used in both ways in this report. We trust the context in each instance makes clear the way in which the term is used.

[85] Zinnbauer, D. et al, *eInclusion Vision and Action: Translating vision into practice*, vision paper, IPTS, Seville, 2006.

3 THREATS AND VULNERABILITIES

In this chapter, we present a review of threats and vulnerabilities that could afflict society and individuals in the AmI world. As will be apparent in the pages that follow, we foresee that many of the threats and vulnerabilities that afflict us now will also afflict the AmI world. Or, to put it differently, based on our research so far, we have discovered few threats and vulnerabilities that could be described as unique or new. To be clear about this, we mean *classes* or *types* of threats and vulnerabilities. In saying so, we do not in any way mean to assuage the AmI enthusiasts. It's been said that, if left unchecked, AmI could obliterate privacy[86], but this is not a *new* threat. Our privacy has been eroding for a long time. By the time, a full-blown, all-singing, all-dancing AmI world is truly upon us, there may not be much left to obliterate. Similarly, it's been argued (and is argued in our reports too) that AmI threatens the individual with a loss of control – if an intelligent environment surrounds us, we may cede much of our control over it to the intelligence embedded everywhere. But this loss of control phenomenon is not new either. We have already ceded a lot of control over our lives to the government and the corporate warlords who pillage consumer society today. What is different about AmI is the scale of the data that will be available. When everything is embedded with intelligence, when AmI is pervasive, invisible, ubiquitous, when everything is connected[87] and linked, the threats and vulnerabilities that we know today will become even greater risks than they are now.

3.1 DISTINGUISHING BETWEEN THREATS & VULNERABILITIES

Unless adequate safeguards are implemented, the diffusion of AmI applications will entail a number of negative side effects and even risks, which, if not addressed, will most likely jeopardise the potential economic and social benefits of the technology. Prior to the formulation of appropriate safeguards and policy options, a better understanding of AmI's unwanted consequences needs to be developed. Analytically, the potential dangers associated with AmI systems can be differentiated between threats and vulnerabilities.

SWAMI's use of these the terms are based on definitions presented by the Special Interest Group 2 "Security and Trust" of the Wireless World Research Forum, on the standards established by ISO 17799[88] and ISO 13335[89] and on the Future Threats and Crimes (FTC) study performed for IPTS[90].

---

[86] Brey, Philip, "Freedom and privacy in Ambient Intelligence", *Ethics and Information Technology*, Vol. 7, No. 3, 2005, p. 165.

[87] Cf O'Harrow, p. 107: "We have created a unique identifier on everybody in the United States," said [Ole] Poulsen, the company's [Seisint Inc.] chief technology officer. "Data that belongs together is *already* linked together." *[Italics added.]*

[88] ISO/IEC 17799:2005(E): Information technology – Security techniques – Code of practice for information security management. Second edition. International Organization for Standardization, Geneva, 15 June 2005. www.iso.org.

[89] ISO/IEC 13335-1:2004: Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, International Organization for Standardization, Geneva, 2004. www.iso.org.

[90] Qinetiq, Transcrime and Interpol, *Future Threats and Crimes in the Ambient Intelligent Environment*, study for IPTS, 2005.

- A **vulnerability** is a flaw or weakness in a system's design, its implementation, or operation and management that could be exploited to violate the system and, consequently, cause a threat. Vulnerabilities may have different dimensions: technical, functional or behavioural.
- A **threat** is the potential for one or more unwanted consequences caused by a circumstance, capability, action, or event that could be harmful to a system or person. Threats can be caused naturally, accidentally or intentionally. In essence, a threat is a ubiquitous phenomenon.[91]

However, these threat and vulnerability definitions have been somewhat adapted to the context of this study. Effectively, the ISO definitions focus on security aspects of software systems. In this study, we concentrate not only on security but on other aspects as well, such as privacy, identity, and trust and generally on all AmI devices and technologies. In addition, special emphasis is put on the user because of AmI's user centric approach, which constitutes an important element of the study's context.

The threats and vulnerabilities, which will be outlined in the following sections, have been rounded up from various sources dealing more or less directly with ambient intelligence: studies, reports, projects and stories in the press have been used to identify negative side effects and dangers associated with existing and future AmI applications. Moreover, we make references to situations from the dark scenarios in SWAMI's second report[92] in order to illustrate numerous threats and vulnerabilities.

It should be noted that some threats and vulnerabilities afflict different types of AmI technologies, networks, services and applications.

3.2 PRIVACY EXPOSED

Threats to our privacy come from lots of sources. Here are some of the principal ones that affect us today and we can assume will still be threats in an AmI world. Many of these threats are also threats for identity and security.

3.2.1 Threats

Hackers

Today's networks, interconnected by the Internet, frequently are attacked by hackers who engage in spoofing, phishing, denial of service attacks via worms, Trojans, viruses and other assorted malware. Even companies that provide security services have been exposed to breaches in their own security.[93]

---

[91] Xenakis, C., and S. Kontopoulou, "Risk Assessment, Security & Trust: Cross Layer Issues", Special Interest Group 2, 2006, p. 14.

[92] Punie, Y., S. Delaitre, I. Maghiros and D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission, November 2005. http://swami.jrc.es.

[93] Guidance Software -- the leading provider of software used to diagnose hacker break-ins -- has itself been hacked, resulting in the exposure of financial and personal data connected to thousands of law enforcement officials and network-security professionals. In December 2005, Guidance alerted its customers that hackers had broken into a company database and made off with approximately 3,800 customer credit card numbers. In March, data aggregator LexisNexis acknowledged that hackers had illegally accessed information on more

AmI networks will supply data aggregators with massive amounts of data from new sources such as so-called "smart dust" networks, RFIDs and the intelligent software driving the new 4G networks. As the scale of data aggregated expands exponentially, there will probably be an increasing concentration and rationalisation in the industry as well as in the databases of governments intent on national ID schemes featuring biometrics including DNA data. The giants among the AmI data aggregators will undoubtedly present irresistible targets to hackers just as Microsoft does today.

Hacking can have unpleasant results even at the individual level, as Scenario 1 in the second SWAMI report shows…

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).[94] 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.

Function creep

Function creep occurs whenever data are used for a purpose other than that for which they were originally collected. The economic logic behind such activity is obvious. It provides efficiencies and savings in cost and effort. Being able to reuse personal data presents a great temptation to industry. Article 6.1.b of the data protection directive (95/46/EC), however, foresees that personal data must be collected for specified, explicit and legitimate purposes and that they cannot be further processed in a way incompatible with those purposes.[95] Article 6.1.e. states that the personal data must even be deleted once used for the original purpose: "Data must be 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." Thus, in principle, the directive prohibits secondary processing and transfer of personal data. Even so, function creep will continue. It is in the economic and strategic interests, especially if enforcement of the data protection directive is weak (which it is) and if governments themselves are engaged in function creep (which they are). As AmI penetrates our environment and daily regimes, the amassed data will present new opportunities that were not even dreamed of. In some instances, the individual will benefit from greater personalisation of services and lower costs. In other instances, she will find some of the new services encroaching further upon her sense of privacy and the protection of her personal data.

---

than 310,000 consumers, an attack that was later determined to have been launched after hackers broke into computers used by at least two separate police departments. Krebs, Brian, "Hackers Break Into Computer-Security Firm's Customer Database", *The Washington Post*, 19 Dec 2005.

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

[95] 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 on the free movement of such data, *Official Journal* L 281, 23 November 1995. It should be added that article 6.1.b. continues as follows: "further processing of the data for historical, statistical or scientific purposes is not considered as incompatible provided that appropriate safeguards are provided by the Member States whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual."

AmI will give great impetus to function creep. An AmI world is distinguished not just by ambient intelligence, but also by the interoperable networking of heterogeneous devices. It's been said that whatever can be linked together will be linked together, and therein lies the opportunities and temptations for function creep.

Some have suggested that (precautionary) impact assessments should be made of new technologies before they are developed and deployed in order to build in privacy safeguards. But some technologies may be used for new applications not foreseen even after they are deployed.

Surveillance

Many analysts have said the war in Iraq has not reduced terrorism, but only served to stoke it even more. With the growing and ever-present risk of terrorism, governments have become more demanding of information on just about everybody. In the United States, the USA PATRIOT Act has greatly expanded the government's authority to monitor Americans and foreign residents alike.[96]

Lest we in Europe think that we are not subject to legislation as invidious as the PATRIOT Act, Privacy International, a London-based privacy watchdog organisation, has found that on every policy involving mass surveillance of its citizens, the EU is prepared to go well beyond what the US government finds acceptable and palatable, and violate the privacy of citizens.[97]

In December 2005, for example, the European Parliament approved legislation requiring telecom companies and Internet service providers to retain details of their subscribers' phone calls, faxes and e-mail messages for six months to two years.[98] Although they are not required to record the actual content of communications, they must keep track of the date, destination and duration of communications and make details available to law enforcement authorities in the interests of fighting organised crime and terrorism. EU countries have until August 2007 to implement the directive, which was initially proposed after the Madrid train bombings in 2004, when phone and Internet records were used to track terrorists.

The data retention directive shows how unclear the border between private and public authorities has become in the case of law enforcement and security. A case in point

---

[96] Gellman, Barton, "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans", *The Washington Post*, 6 Nov 2005. See also Werther, "The Liberties of the Subject", CounterPunch, 17 Jan 2006. http://www.counterpunch.org/werther01172006.html

[97] "What is Wrong With Europe?", Media Release, Privacy International, 14 Dec 2005. The report is available at http://www.privacyinternational.org/comparativeterrorpowers or http://www.privacyinternational.org/issues/terrorism/rpt/comparativeterrorreportdec2005.pdf. See also Hosein, G., "Threatening the Open Society: Comparing Anti-terror Policies and Strategies in the U.S. and Europe", *Privacy International*, London, 2005. http://www.privacyinternational.org/issues/terrorism/rpt/comparativeterrorreportdec2005.pdf.

[98] This is now binding. See Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L 105 , 13/04/2006 P. 0054 - 0063. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

occurred when the police in the Dutch city of Nijmegen sent 3,000 SMS messages to the people who where in the neighbourhood of a killing that took place one evening. The police asked for collaboration and for recipients to surf to a questionnaire on the police force's website. In another case, the police sent 17,000 SMS messages to all people who were in the neighbourhood of a soccer stadium on 17 April 2005 where some rioting broke out between the fans of the Ajax Amsterdam and Feyenoord Rotterdam football teams.[99]

But the data retention directive is just the tip of a very large iceberg. Surveillance is increasing in the streets, buses, Underground, shops, workplace and on the motorways. Hence, it is now almost impossible to go outside your home without coming under surveillance.

The spectre of a watchful Big Brother looms large in today's society and especially in the press. Stories about the increasing surveillance, especially by government, are frequent. During the American Super Bowl Final in Tampa, Florida, in June 2001, the police used intelligent video cameras with face recognition to scan all 100,000 spectators in the stadium. The faces of these spectators were compared with the facial templates stored in a database of wanted criminals and terrorists.

The government is not the only Big Brother. The falling costs and increasing capabilities of surveillance technologies have allowed parents to watch from a distance what their children are doing. Similarly, employers surveil their employees, neighbours can spy on each other, as can friends and relatives.

Location-based services form a kind of surveillance. Mobile phone operators and industry have developed emergency service telephone numbers (112 in Europe, 999 in the UK and 911 in the United States), which can be activated automatically and which will inform the network of the physical location of the user. New electronic services, such as those offered by uLocate and Wherify Wireless, provide the physical location of mobile phone users.[100]

If the risk of terrorism is growing, then AmI will be most welcomed by those who are supposed to be looking after our security. While AmI technologies will offer benefits in terms of enhancing security (e.g., networked sensors can detect the presence of unauthorised people), they will also present greater threats to our privacy (networked sensors can be employed to keep track of what we are doing or even how we behave in certain situations). Some experts have stated that security and privacy are not necessarily opposite ends of a teeter-totter – as one goes up, the other goes down – but many will not feel that way as we come under increasing surveillance, not just every time we go outside our homes or make a telephone call or sit in front of our keyboards, but as we find ourselves surrounded by products, all with embedded devices.

[99] "Politie stuurt 3000 sms-berichten in onderzoek-Sévèke", Webwereld Newsletter, 21 March 2006, http://www.webwereld.nl/ref/newsletter/40348

[100] Harmon, Amy, "Lost? Hiding? Your Cellphone Is Keeping Tabs", *The New York Times*, 21 Dec 2003. "We are moving into a world where your location is going to be known at all times by some electronic device," said Larry Smarr, director of the California Institute for Telecommunications and Information Technology.

In an AmI society, one can foresee the possibility of extensive use of wearable devices and/or implants, like those that have already been developed.[101] Parents may want to keep track of where their children are, especially if they fear the randomness of crime and terrorism. The same could be said of employers, especially those with employees in companies or organisations that have serious security requirements. Indeed, it is not impossible to imagine a day when almost everyone will have implantable devices, not only for tracking their whereabouts, but also for monitoring their physiological condition. At the same time, there may be considerable social pressure, perhaps even legal requirements, for individuals to bear such implants as a security measure. One could further foresee such implants interacting with the "intelligence"-embedded, networked environment too.

Medical implants that allow for remote monitoring of individuals' well-being could also be subject to abuse where the individual's physiological and/or behavioural reactions in certain situations could be regarded as incriminating. A European Group on Ethics in Science and New Technologies (EGE) has considered the non-medical use of implants and presented its opinion to the European Commission.[102] An EC-funded project (BITE) is also considering such issues.[103]

AmI devices such as implants or technologies that monitor our physiological condition and behaviour could well make our society more secure, particularly if they enable law enforcement authorities and intelligence agencies to take preventive measures. Preventive actions by the police are featured in the *Minority Report* film, but is this the kind of society we want? More control in order to prevent criminal acts, detect offenders and punish them may be counterproductive for society as a whole. In 1968, the philosopher Heinrich Popitz wrote a classic text on the "preventive effects of nescience" in which he argues that too much (precautionary) knowledge destabilises society, leads to a climate of distrust and finally to more instead of less crime. A world where every breach of the rule is detected and punished can only be hell.

Profiling

Companies such as Amazon keep track not only of their customers purchases, but also their browsing, and with the accumulation of such data, they can build up increasingly accurate profiles of their customers in order to offer them other products in which they might be interested. Search engines keep a log file that associates every search made on its site with the IP address of the searcher. And Yahoo uses similar information to sell advertising; car companies, for example, place display advertising shown only to people

[101] A US company, Applied Digital Solutions, has developed something called a VeriChip which, it says, is about the size of a grain of rice, and is the world's first "subdermal, radio frequency identification (RFID) microchip". See "Children to be chipped in Mexico", Out-Law.com, 13 Oct 2003. See also Libbenga, Jan, "Video surveillance outfit chips workers", *The Register*, 10 Feb 2006. http://www.theregister.co.uk/2006/02/10/employees_chipped: "A Cincinnati video surveillance company CityWatcher.com now requires employees to use Verichip human implantable microchips to enter a secure data centre… Although CityWatcher does not require its employees to take an implant to keep their jobs, they won't get in the data centre without it." *The New Yorker* reported the case of one individual who had an RFID implanted between a thumb and forefinger so that he could pass his hand in front of his computer and have the computer's security system recognise his password. He bought his tag online, from a company called PhidgetsUSA, for $2.50. Wilkinson, Alec, "Taggers", *The New Yorker*, 20 Mar 2006.

[102] The EGE is an independent group, which advises the Commission on how ethical values should be taken into consideration in the regulation of scientific and technological developments. http://europa.eu.int/comm/european_group_ethics/avis3_en.htm

[103] http://www.biteproject.org/ BITE is the acronym for Biometric Information Technology Ethics.

who have entered auto-related terms in Yahoo's search engine.[104] Companies such as Doubleclick are specialised in building and analysing profiles by placing cookies on our personal computers and keeping track of our surfing behaviour across numerous affiliated websites.

Customer-supplied data, the data obtained from monitoring purchasing habits and surfing behaviour, and the data obtained from third parties, can also be used to implement dynamic pricing and behavioural targeting. Dynamic pricing, a modern incarnation of price discrimination, means that different prices are offered to customers based on their characteristics. [105]

The unbounded use of personal data for profiling purposes easily leads to self-fulfilling prophecies. People will only see the choices presented to them on the basis of their profile, which leads to choice within these boundaries, and this in turn may lead to refinements in their profile.[106]

From Scenario 4, second SWAMI report

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?

Use of the same identifier across multiple transactions can yield comprehensive profile information to the service provider on the usage, interests or behaviour of the user, by linking all available information, possibly from both the online and offline worlds. [107]

Some organisations engage in data mining, rather than profiling in the above sense, as they look for suspicious patterns of behaviour. NSA technicians, besides actually eavesdropping

[104] Hansell, Saul, "Increasingly, Internet's Data Trail Leads to Court", *The New York Times*, 4 Feb 2006.
[105] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 10.
http://www.prime-project.eu.org/public/prime_products/deliverables/
For a practical example of how mobile phone companies engage in differential pricing, see Richtel, Matt, "Suddenly, an Industry Is All Ears", *The New York Times*, 4 March 2006: "When a [Cingular call centre] representative answers the phone, an information page pops up that includes the caller's name and number, whether he or she has called in the last five days, and why that call was made. In the top right of the screen are two icons — one indicating whether the caller is a threat to quit service (largely a measure of whether the customer is still under contract), and the other showing how much money the caller spends each month (a measure of the customer's value). Before long, the screen indicates if the customer is profitable. If a customer is not very profitable, the company may be less likely to make concessions."
[106] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 11.
http://www.prime-project.eu.org/public/prime_products/deliverables/
[107] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 14.
http://www.prime-project.eu.org/public/prime_products/deliverables/

on specific conversations, have combed through large volumes of phone and Internet traffic in search of patterns that might point to terrorism suspects.[108]

Out of a soup of (cellular) phone traffic, financial traffic and Internet traffic, relationships are detected by the presence of keywords, voice prints or characteristic financial transactions, but questions have been raised about who is making the decisions about what sorts of indicators and patterns are used to trigger human attention. The power of intercept technologies and data mining software and the lack of oversight enable investigations of all sorts of things with minimal or no oversight.[109]

From Scenario 4, second SWAMI report

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

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

Security expert Bruce Schneier has pointed out flaws with profiling schemes. "Profiling has two very dangerous failure modes. The first one is … the intent of profiling … to divide people into two categories: people who may be evildoers … and people who are less likely to be evildoers... But any such system will create a third, and very dangerous, category: evildoers who don't fit the profile… There's another, even more dangerous, failure mode for these systems: honest people who fit the evildoer profile. Because actual evildoers are so rare, almost everyone who fits the profile will turn out to be a false alarm. This not only wastes investigative resources that might be better spent elsewhere, but it causes grave harm to those innocents who fit the profile… profiling harms society because it causes us all to live in fear...not from the evildoers, but from the police… Identification and profiling don't provide very good security, and they do so at an enormous cost. Dropping ID checks completely, and engaging in random screening where appropriate, is a far better security trade-off. People who know they're being watched and that their innocent actions can result in police scrutiny are people who become scared to step out of line. They know that they can be put on a 'bad list' at any time. People living in this kind of society are not free, despite any illusionary security they receive."[110]

[108] Lichtblau, Eric and James Risen, "Spy Agency Mined Vast Data Trove, Officials Report", *The New York Times*, 24 Dec 2005.
[109] Tomlinson, Christine, "When Bush's Eavesdroppers Get a False Positive", CounterPunch, 9 Feb 2006. http://www.counterpunch.org/tomlinson02092006.html
[110] Schneier, Bruce, "Identification and Security", Crypto-Gram Newsletter, 15 Feb 2004. http://www.schneier.com/crypto-gram-back.html. George Clooney provided us with a recent reminder of this in his recent film, *Good Night and Good Luck*, about Joe McCarthy, who professed that he was making America more secure by exposing Communists and their sympathisers, when in reality he was instilling fear and paranoia across society.

The PRIME project has echoed this sentiment: Unbridled data collection and profiling by the State in the name of protecting (national) security may lead to unjust and ultimately unwarranted blacklists, however noble the intentions may be. This happens not only in totalitarian regimes, but also in free societies.[111]

The European Network of Excellence FIDIS has a work package devoted to profiling, as this seems the nexus of a set of emerging technologies (RFID systems, adaptive ubiquitous computing, smart dust, identity management systems).[112] The importance of profiling as a precondition for AmI demands a thorough investigation of its implications. To understand the impact of profiling, one must acknowledge the fact that it consists of a new type of knowledge, rather than just information.[113]

3.2.2 Vulnerabilities

In addition to the threats highlighted above, privacy today is subject to various vulnerabilities, among which are the following.

Lack of public awareness or concern about privacy rights

Many people are unaware of their rights and feel unable to know what actually happens to their data. This is not surprising, given the opacity of the processes. This is a serious vulnerability since it is a vulnerability that cannot be fixed or addressed until someone becomes aware of it (and exposes it).

Lack of public awareness is one thing, but lack of concern about one's rights or a willingness to trade off some of one's civil liberties for greater security is quite another. Recent public opinion polls published in the US suggest that a majority of the public is not really that concerned about encroachments on their privacy and civil liberties, that they are of view that giving up some privacy or forsaking some of their civil liberties is the price of countering security threats, especially from terrorists.[114]

While one could understand a certain public acceptance in trading off privacy for better security (if one believes one's political leaders, law enforcement authorities and intelligence agencies), many citizens are willing to forsake their privacy for much less than their own perceived personal safety. Exhibitionists (with videocams in their bedrooms) can

---

[111] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 11.
http://www.prime-project.eu.org/public/prime_products/deliverables/

[112] A set of deliverables that provide an extensive analysis of profiling and its far-reaching implications is available at www.fidis.net. See Hildebrandt, M. & J. Backhouse, Descriptive analysis and inventory of profiling practices, FIDIS deliverable 7.2, Brussels, 2005; M. Hildebrandt & S. Gutwirth (eds.), *Profiling: Implications for Democracy and Rule of Law*, FIDIS deliverable 7.4, Brussels, 2005; Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence, FIDIS Deliverable D7.3, Brussels, 2005.

[113] Hildebrandt, M., "Profiles and correlatable humans", in N. Stehr (ed.), *Who Owns Knowledge?* New Brunswick NJ, Transaction Books, 2006. See also Custers, Bart, *The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen, 2004.

[114] Drees, Caroline, "Civil liberties debate leaves much of America cold", Reuters, published in *The Washington Post*, 18 May 2006.

be found in the cyber world as they can be in the real world. People post their CVs and much else on the Internet without much regard for their personal privacy.[115]

Lack of enforcement and oversight of privacy rights

Most people are not even aware that data protection infringements are taking place. If they know or presume that infringement is taking place, they often just don't react (e.g., spam). And even if they do react and want to enforce their rights, most EU legal systems require that their damage must be proven.

Some of our personal data are held by the governments and organisations in our own countries, and some are held in other countries. Some countries may have legislation or regulation that affords relatively good protection of our privacy, while others may have regimes that offer no protection whatsoever.

No matter what the best of the legal regimes say, the complexity of the regulation, incomplete enforcement, and sometimes even conscious decisions by businesses and governments not to comply with the rules render legislation ineffective.[116]

An instance of the latter came to light in the United States in December 2005 when *The New York Times* published (after sitting on the news for up to a year) an article about the National Security Agency conducting a domestic surveillance operation without court-approved warrants.[117] One commentator has said that there are three issues pertaining to the NSA's domestic surveillance program that should be of great concern to all citizens. These issues are:

- intrinsic violations of privacy by the very nature of the technology of the program,[118]
- collateral damage in the execution of the program,[119]
- lack of oversight in the choice of targeting of the surveillance program. [120]

Erosion of rights and values

The erosion of the right to privacy in the past century has been subtle, incremental, gradual and as relentless as technological advance. In today's surveillance society, where our personal data are not secure and are mined monitored and captured, people have

---

[115] "Privacy has now become a tradeable commodity. Commercial firms offer consumer schemes in which consumers get to trade in personal data in exchange for discounts or free goods. Many consumers find this an acceptable practice. It could be argued that technically, such practices do not involve violations of privacy, since authorizations have taken place. Yet, such authorizations are often given on the basis of a very limited understanding of what personal information is collected and how it would or could be used. It is therefore often doubtful that such authorizations are based on informed consent." Brey, Philip, "Freedom and privacy in Ambient Intelligence", *Ethics and Information Technology*, Vol. 7, No. 3, 2005, p. 165.

[116] [PRIME] Hansen, Marit and Henry Krasemann (eds.), Privacy and Identity Management for Europe – PRIME White Paper, Deliverable D 15.1.d, 18 July 2005, p. 12.
http://www.prime-project.eu.org/public/prime_products/deliverables/

[117] Risen, James and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *The New York Times*, 16 Dec 2005.

[118] This is the "warrantless" surveillance aspect of the program.

[119] Some (most?) of these intercepts will be false-positives – they will turn out to be innocuous – and this is one of the real dangers of the program – collateral damage in the intelligence operation: Otherwise innocent persons can be misidentified as targets of interest.

[120] Tomlinson, Christine, "When Bush's Eavesdroppers Get a False Positive", CounterPunch, 9 Feb 2006. http://www.counterpunch.org/tomlinson02092006.html

surrendered the right to be let alone in the interests of greater security. For the most part, people have accepted the arguments of law enforcement and intelligence agencies that privacy has to be circumscribed so that they have the tools they need to apprehend criminals and terrorists and to combat the malicious code that floats around the Internet.

Perhaps most people view privacy as a right that can be sacrificed, at least to some extent, if it leads to greater security. But there are questions whether it *has* led to greater security, questions that are unlikely to be adequately answered before the widespread deployment of AmI networks in the near future.

Some have argued that privacy is fundamental to democracy, whether people recognise it or not. In addition to privacy, values such as autonomy (sovereignty), human dignity, physical and mental integrity and individuality are easily undermined by advanced methods of personal data collection, profiling and monitoring. Other fundamental rights – part of the European Charter of Fundamental rights – can be under pressure in an AmI world without privacy or with just a minimal level of privacy, such as the freedom of thought (brain research shows that neural signals can be transformed into computer data and transmitted over networks), freedom of expression and information (the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers), freedom of assembly and association (location data can reveal assemblies, communication data can reveal associations), the right to education (computer education could become more valuable than alphabetic education), non-discrimination (as a consequence of profiling), integration of persons with disabilities (who have less privacy as a (avoidable) consequence of the system design, and so on.

It is questionable whether the erosion of privacy can be stopped and turned back anymore than shorelines can be recovered after they've eroded away. A somewhat related issue is how much value people will attach to their privacy in an AmI world. Undoubtedly Warren and Brandeis would be shocked to see how the right to be let alone has diminished in the past century and even more shocked to see what little value people attach to their privacy. After some years of experience of living in an AmI world, most people will probably care less than they do even today. But how much or how little they care will probably also be a direct function of how their privacy, their personal data, their communications are abused and/or to what extent they have ulterior motives for minimising their exposure to the authorities (i.e., they really may be criminals or terrorists). Press reports of abuse, of liberties taken with existing laws and constitutional rights must help to stimulate some unease in our society generally, if not outrage by civil liberties groups.

Uncertainties about what to protect and about the costs of protection

Just as privacy is an unstable notion, so it is almost impossible to know what to protect in all contexts, especially in view of the capabilities of data mining and powerful software that can detect linkages that might not otherwise be apparent.

In addition, people's views of privacy keep changing. As noted elsewhere, people are willing to give up some of their privacy for greater security, especially in the aftermath of a terrorist incident.

With the emergence and deployment of AmI networks, the amount of data that can be captured from all sources will expand exponentially by many orders of magnitude. Hence, the cost of providing 100 per cent privacy protection may be prohibitive and unrealistic, even if there were some consensus about exactly what it is we wish to see protected.

Haven't psychologists argued that forgetting is as important as remembering for one's sanity? That could be true for the society as a whole as well.

Uncertainties about the economic costs of privacy erosion

There have been few studies aimed at analysing the value of privacy, either from a corporate point of view or that of the individual. The cost of losing privacy is twofold: On the one hand, one is confronted by the cost of becoming transparent; on the other, one is exposed to the cost of losing control. There is also the cost of new AmI-related crimes such as identity theft. The economic costs, therefore, are not only the design of the system, but also the consequence of the design in the long term (e.g. when you become dependent on software, you need to update, processing systems are replaced after a few years only, and so on).

Certainly, protecting personal data, through security measures, notably in compliance with the EU's data protection directive (95/46/EC), carries a cost. The directive requires data controllers and processors to protect personal data in proportion to "the risks represented by the processing and the nature of the data to be protected" (Article 17.1). Such costs might include the cost of encryption and establishing a range of protection measures, not least of which is training staff. The cost of implementing the information security measures detailed in ISO 17799 could be quite substantial. From a shareholder's point of view, these costs of protecting can be identified, but the value of doing so might be more uncertain. Where's the payback, they might well ask.

There might be some payback in the context of the company's image, i.e., it could say that it complies with ISO 17799 and, accordingly, it might hope or have some expectation that doing so will engender more trust and loyalty on the part of its customers in the company's brand. Even so, doubts must remain as to whether that automatically translates into greater market share or additional profitability. If the company does gain greater market share or additional profitability, the cause might not be the fact that it has taken adequate measures to protect the personal data it holds, but some other factor. As a minimum, the company would need to do some careful market studies to determine what factors led to improvements in its market position.

Some indication of the economic value of privacy can be adduced from the costs borne by companies where there have been breaches of their databases resulting in the theft of personal data. In such cases, companies have had to bear the cost of informing users or subscribers of the breach, of compensating those whose personal data have been compromised, of establishing improved countermeasures, subjecting themselves to independent privacy audits and so on. Recently, ChoicePoint was subjected to a $10 million federal fine over security breaches that exposed more than 160,000 people to possible identity theft. "The message to ChoicePoint and others should be clear: consumers' private data must be protected from thieves," FTC Chairman Deborah Platt

Majoras said.[121] Such direct costs are only part of the overall cost equation, however. There are additional costs arising from, for example, damage to the company's image, reputation and name.

If companies have difficulty in assessing the value of their privacy protection measures, the individual is almost surely faced with even greater difficulties. If the individual is being spammed a lot, getting a lot of unwanted e-mail, how easy or difficult will it be to translate the nuisance it causes into cold hard cash? Is it simply the cost of the individual's time in deleting unwanted e-mail? Can a value be ascribed to the anguish the individual might feel in knowing that his contact details are on some spammer's e-mail list?

Those who have been victims of identity theft might have some pretty good ideas of the costs to them, in terms of lost time and perhaps direct financial loss, in trying to recover from the theft, but still there must be an open question about the stress and anguish caused by the theft and what is the monetary value of such stress and anguish.

Certainly there are social costs too arising from identity theft, but there appears to be no study analysing the costs, even though the number of victims seem to be rather large. The US Federal Trade Commission has estimated the number of victims at around 10 per cent of the population, and the number of victims in the UK, if not the EU as a whole, also has been estimated as increasing, if not to such levels.

While the costs of identity theft can be estimated, what is one to say about the costs of, for example, increased surveillance? How does the individual value the supposed increase in security versus the encroachment upon his privacy?

For the individual the value of his personal data must be even more difficult to pin a figure to. For starters, the individual is highly unlikely to be aware of all those organisations that hold some of his data. And even if he were, he would most likely able to judge the cost to him of some threat to his privacy arising from the data mining operations and the linkages aimed at either providing him with more personalised services or establishing his culpability in the context of some supposed terrorist threat.

And what of the future? How easy will it be to place a value on what remains of our sense of privacy in 10 years time, assuming encroachments continue, compared to the value that might be ascribed today? Is there a formula that can be devised to work out the net present value of privacy today compared with that in the AmI world a decade hence?

Lax security

One of the most serious vulnerabilities facing those who care about their privacy is the lax security put in place to protect personal data and the privacy of communications. A quarter of UK businesses are not protected against the threat caused by spyware, while spyware caused one in seven of the security incidents reported, according to a recent report by the Department of Trade and Industry.[122]

---

[121] Mohammed, Arshad, "Record Fine for Data Breach", *The Washington Post*, 27 January 2006.

[122] Espiner, Tom, "Viruses cause most security breaches", ZDNet UK, 28 Feb 2006. http://news.zdnet.co.uk/0,39020330,39254929,00.htm. Chris Potter, co-author of the report and partner at PricewaterhouseCoopers, said spyware was the hardest threat to detect. He is quoted as saying "Old style

This vulnerability has at least two aspects – one is the increasing sophistication of efforts by hackers, industry and government to acquire or mine personal data unlawfully or to intercept communications. The other is the inadequate measures taken by those who are expected to protect personal data and the privacy of communications.

Reports of Internet service providers and telecommunications companies providing details at the behest of government give cause for alarm. Protests by telecom companies against the data retention directive were not altruistic. Rather they were concerned about the impact on their bottom lines, about the cost of storing data and records for longer than necessary or longer than required by the 2002/58/EC directive. Google has won plaudits for resisting efforts by the US Department of Justice to have access to its search logs. In its rebuttal of the DOJ subpoena, Google said that if it were forced to hand over the data, it would "compromise its principles". The company maintains that "Google will, without a doubt, suffer a loss of trust among users." It also raised the fear that government investigators might come across personal data through user-initiated searches for their own social security or credit card numbers.[123] The other major search engines – MSN, Yahoo and AOL – have already turned over the data requested by the government.

The prevalence of identity theft in part reflects the failure of many information brokers, retailers and credit issuers to adequately protect records or to do enough to stop criminals who seek them by verifying their identities.

If some good can be seen coming from the many instances of abuse of personal data held by the private sector and government, it is that security issues have become of greater concern to those who are designing and building the AmI networks of the future. On the other hand, offsetting that design awareness is an assumption that future networks are likely to be much more complex than those in place today. And with each additional complexity, there is the potential for exploiting those complexities with malicious intent.

Government and industry are less than forthright

So many people and organisations hold personal data about us, it is virtually impossible to know who they are, let alone to keep track of what they are doing with our data, whether the data they hold are accurate, and how such data may change, be added to, deleted or amended – even though, according to EU data protection legislation, data processors are supposed to notify national authorities of the categories of data processed, the purpose of processing, the retention period and the security and confidentiality measures taken and even though data controllers are expected to notify individuals concerned so that they can access, amend or delete the data. Although these obligations exist, their efficacy has been undermined by the bad faith of some private sector data controllers and because enforcement has not been rigorous.

Corporate concerns about their companies' share prices can undermine legal obligations on disclosure, as shown in Scenario 3 from the second SWAMI report.

attacks just caused indiscriminate damage, like a plane dropping bombs. Now it tends to be a mass of guerrillas attacking organisations to take confidential information, which is much more subtle and insidious."

[123] Malone, Steve, "Google preps privacy defences", *PCPro*, 20 Feb 2006. http://www.pcpro.co.uk/news/83794/google-preps-privacy-defences.html

Max Court, DMC's general counsel, spoke up. "If we were exposed? Are you suggesting we should withhold information about this theft from the police and those whose files have been copied?"

"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."

We should not be surprised by comments made by executives of two major data brokers who acknowledged to a US Senate panel that their companies did not tell consumers about security breaches that occurred well before recent incidents exposed more than 400,000 people to possible identity theft.[124] Similarly, governments, notably the Bush administration, have been reticent about domestic surveillance even after *The New York Times* exposed the fact that the US National Security Agency had been spying, without warrants, on thousands of Americans.

3.3 THREATS AND VULNERABILITIES IN IDENTITY

3.3.1 Threats to identity

Threats to our identity can come from various sources, among which are the following.

Identity theft

Identity theft (or identity-related crime) is one of the fastest-growing white-collar crimes. Typically someone steals our financial details, most often our credit card details, to commit fraud. The identity thief can impersonate us financially, to take out loans, to raid our bank accounts, to purchase luxury items. The credit card companies may minimise our losses when purchases are made against our cards (or some facsimile thereof), but we may be liable for the other items. Identity theft can also ruin our creditworthiness even if we are not culpable. It may take a long time, a lot of aggravation, to restore our creditworthiness and recover our financial identity.[125] As serious as identity theft is for us as individuals, the credit card companies feel no less aggrieved and, given the magnitude of identity theft, they have been devoting lots of resource and effort to deal with it. The recent replacement of our signature by chip and pin cards is just one indication of their efforts to combat this form of fraud.

Identity theft can also occur in the home, as depicted in Scenario 1 from the second SWAMI report…

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.

[124] Krim, Jonathan, "Consumers Not Told Of Security Breaches, Data Brokers Admit", *The Washington Post*, 14 April 2005. See also Stout, David, "Data Theft at Nuclear Agency Went Unreported for 9 Months", *The New York Times*, 10 June 2006.

[125] A survey conducted by Privacy Rights Clearinghouse and the California Public Interest Research Group found that the average victim of identity theft did not find out that he or she was a victim until 14 months after the identity theft occurred and that it took the victim an average of 175 hours to solve the problems that occurred as a result of the identity theft. Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, p. 99.

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.

Although identity theft can be performed in lots of ways, including rifling through other people's rubbish for discarded credit card and bank account statements, the Internet has become a home for ID miscreants. Internet scams leading to ID theft include spam e-mails containing viruses that access information on computers, and practices known as "phishing" that use e-mail messages to lure unwitting consumers to Web sites masquerading as home pages of trusted banks and credit card issuers. Online visitors are then induced to reveal passwords as well as bank account, social security and credit card numbers.

The profitability of identity theft is highlighted in Scenario 3 from the second SWAMI report…

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. 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.

Many more Americans have been victims of identity theft than Europeans, although identity theft is rising fast in Europe. The US Federal Trade Commission said 27.3 million Americans had their identities stolen from April 1998 to April 2003 – with more than a third of them, or 9.9 million, victimised in the last 12 months of that period alone. The crimes ranged from the theft of a credit card number to more elaborate identity thefts used to secure loans. During those 12 months, the report said, businesses and financial institutions suffered about $48 billion in losses because of identity theft, and victimised consumers paid more than $5 billion in out-of-pocket expenses to regain their financial identities.[126]

A much smaller number of UK citizens, even on a percentage are affected by identity theft. The UK Home Office says more than 100,000 people are affected by identity theft each year.[127] Identity fraud is estimated to cost the UK economy about £1.7 billion.

Meanwhile, identity fraud is costing the credit card sector billions of euros each year, and is a major source of privacy complaints.[128] Both MasterCard and Visa monitor Web sites

[126] O'Brien, Timothy L., "Identity Theft Is Epidemic. Can It Be Stopped?" *The New York Times*, 24 Oct 2004. A more recent (2006) study by Javelin Strategy & Research shows that the number of identity-fraud victims in the US fell to 8.9 million from 10.1 million in 2003. The cost to victims, however, was up, to $56.6 billion from $53.2 billion in 2003. http://www.javelinstrategy.com

[127] http://www.identity-theft.org.uk/

that broker stolen credit card numbers and other personal information they've discovered that an identity is worth about $10 on the Internet. [129]

Despite the prevalence of identity theft, prosecutions are rare, and police investigations – when they do happen – are time-consuming, costly and easily stymied. A 2003 study by Gartner Inc. suggested that an identity thief had about a 1 in 700 chance of getting caught.[130]

It is an open question whether ambient intelligence will increase or decrease opportunities for identity theft and fraud. With orders of magnitude of more personal information generated in an AmI environment, one might not be too hopeful that the problem will go away. On the other hand, if some privacy enhancing technologies, like those proposed in the PROGRESS Embedded Systems Roadmap or in the PISA and PRIME projects, are developed and become widely available, one might think the consumer will have better defences against at least some forms of identity theft.[131]

But technology can only help to some extent. Gullibility and carelessness, human traits, are less easily fixed.

Function creep

The data protection directive 95/46, which is not applicable in areas of criminal law and state security, defines an identity and any information related to an identified or identifiable *natural* person as personal data. Identification is the processing of personal data and therefore falls under the principles of data protection such as the principle of purpose specification and use limitation (use conforms only to the original purpose).

The growing awareness of identity theft has prompted many businesses to require customers to provide identification information, especially online and over the telephone. Identification information can come from passports or ID cards or drivers' licences as well as biographical data such as date of birth or mother's maiden name or from biometrics like fingerprint or iris scans. In attempts to minimise the risk of identity theft and fraud, businesses may be increasing privacy risks.

---

[128] The FTC said identity theft again topped the number of consumer complaints it received in 2005, as it has in recent years. See FTC press release "FTC Releases Top 10 Consumer Fraud Complaint Categories", 25 Jan 2006. http://www.ftc.gov/opa/2006/01/topten.htm. See also Krim, Jonathan, "Data on 3,000 Consumers Stolen With Computer", *The Washington Post*, 9 November 2005. "Social Security numbers and other information about more than 3,000 consumers were stolen recently from TransUnion LLC, one of three U.S. companies that maintain credit histories on individuals, in the latest of many security breaches that have focused congressional attention on identity theft and fraud."

[129] O'Brien, Timothy L., "Identity Theft Is Epidemic. Can It Be Stopped?" *The New York Times*, 24 Oct 2004.

[130] Zeller, Tom Jr, "For Victims, Repairing ID Theft Can Be Grueling", *The New York Times*, 1 Oct 2005.

[131] The term privacy-enhancing technologies (PETs) represents a spectrum of both new and well-known techniques to minimise the exposure of private data, for users of electronic services in the information society. Currently, no widely accepted definition of privacy-enhancing technologies has been established, but one can distinguish technologies for privacy protection (psydeunomizer, anonymizer and encryption tools, filters, track and evidence erasers) and for privacy management (informational and administrational tools). See e.g. Koorn, R., H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen and J. Borking, "Privacy-Enhancing Technologies. White Paper for Decision-Makers", The Hague, Ministry of the Interior and Kingdom Relations, 2004. http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

Even if the choice is made to implement authentication systems only where people *today* attempt to discern identity, the creation of reliable, inexpensive systems will invite function creep – the use of authentication systems for other than their originally intended purposes – unless action is taken to prevent this from happening. Thus, the privacy consequences of both the intended design and deployment and the unintended, secondary uses of authentication systems must be taken into consideration by vendors, users, policy makers and the general public. [132]

It is not hard to see signs of function creep when we travel from one country to another. The US, the UK, Japan and other countries are introducing biometric requirements to supplement passport data. The UK has introduced iris scanning, supposedly to speed passengers through immigration controls. The scan is linked to their passport details. Now the government will have one more bit of data about UK and other citizens who chose to participate in the scheme. For its part, Japan, like the US, has decided to fingerprint and photographs visitors. Gathering such biometric data is grist, not just for civil aviation authorities, but also for law enforcement, the intelligence agencies and controlling immigrants. It's the same with loyalty cards that supermarkets foist on their customers. Such cards are purportedly to reward loyal customers when in reality they serve the market research and marketing departments. Such cards strip away the anonymity of cash-paying customers, enabling the supermarket chains to better target and spam customers.

As AmI becomes pervasive, at least in developed countries that can afford such networks, the opportunities for supplementing basic identifier data will surely grow.

Among examples of function creep, typically related to AmI environments and applications, are the following:

- RFID tags that are used to facilitate the supply chain are used after the point of sale to identify objects.

- Biometric data processed for verification or identification purposes may reveal medical conditions. Correlations between papillary patterns and diseases such as leukaemia and breast cancer exist.[133] Face recognition can reveal racial or ethnic origin.[134]

- Cookies, used to facilitate web access and enhance user comfort (setting the right language, remembering passwords, etc), can be used for profiling purposes.

- Intelligent cameras to control roads and signal traffic jams can be used to look out for cars whose owners did not pay traffic tax. Private companies could 'rent' the equipment of the government to look for subjects and objects, and vice versa.

[132] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, p. 29.
[133] The Article 29 Data Protection Working Party opinion on Council regulation 2252/2004 refers to the FIDIS study on PKI and biometrics (page 68) and states: "In the case of storing fingerprints attention will have to be paid in so far as various correlations between certain papillary patterns and corresponding diseases are discussed. As for instance certain papillary patterns are said to depend on the nutrition of the mother (and thus of the foetus) during the 3rd month of the pregnancy. Leukaemia and breast cancer seem to be statistically correlated with certain papillary patterns. Any direct or precise correlations in these cases are not known…".
[134] Article 29 Data Protection Working Party, *Working document on biometrics*, 10.

Exploitation of linkages by industry and government

Even among those who understand the benefits of partial identities, it will be miraculous if they can avoid usage of at least one attribute across those partial identities. Only one attribute shared by two partial identities is needed to establish a link between them and all the other attributes. It could be a telephone number, an e-mail address, a date of birth, almost anything will do.

An AmI world will be a highly networked world, which will facilitate linkages between different networks. Hence, where today it is possible to have multiple partial identities that correspond to our different roles in society – as neighbour, employee, student, etc – AmI will facilitate linkages between these different partial identities leading to a great increase in their integration. Both government and industry, despite any protests to the contrary, will find it irresistible to facilitate such linkages for their own, sometimes nefarious, purposes. The more linkages that can be established, the more government and industry will know about us, our behaviour patterns, what we are doing, where we are at any given moment, our disposition towards particular products or services or activities some of which may be deemed as socially unacceptable.

From the individual's point of view, however, more linkages will raise more concerns about the security and protection of our personal data. It may also lead to an erosion of trust – how much trust are we likely to place in Big Brother and a host of "little brothers" when we feel they know almost as much about us as we do ourselves.

Penetration of identity management systems (hacking, spoofing, DOS, etc)

Identity management systems are subject to many of the attacks common to other Internet or computer-communications-based systems, such as hacking, spoofing, eavesdropping and denial of service.

Some authentication systems make it possible to identify an individual without the individual's consent or even knowledge. Such systems deny the individual, and society, the opportunity to object to and to monitor the identification process. These technologies are particularly vulnerable to misuse because their use is hidden.[135]

There's no reason to think these sorts of attacks that plague us today are likely to go away in an AmI world.

3.3.2 Vulnerabilities in identity

In addition to the threats mentioned above, identity management systems may exhibit certain vulnerabilities, such as the following.

Authentication may intrude upon privacy

A US National Research Council report has warned that authentication technologies could intrude upon privacy in different ways. Authentication methods may require contact with or close proximity to the body, potentially raising concerns under the "bodily integrity"

[135] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, pp. 30-31.

branch of privacy law. Authentication may introduce new opportunities to collect and reuse personal information, intruding on "information privacy". Authentication systems may be deployed in a manner that interferes with individuals' "decisional privacy" by creating opportunities for others to monitor and interfere with important expressive or other personal activities. Authentication methods may raise new opportunities to intercept or monitor a specific individual's communications, revealing the person's thoughts and the identities of the individuals with whom he or she communicates.[136]

Complexity of identity management systems

Governments and industry have been developing a multiplicity of identity management systems for various purposes, with the intent of putting more (or virtually all) of their services online or, in the instance of the rationale for national ID cards, for combating fraud and terrorism. Some systems, for example, the UK's Inland Revenue system that permits individuals to file their tax returns online, are becoming very big indeed with millions of files. Eventually the national ID card scheme will become even bigger. If common standards are agreed for national ID systems across the EU, an EU ID card may not be long in coming. Inevitably, as the systems and their attendant databases become bigger, the complexity of the systems grows.

The multiplicity and complexity of such systems offers a possible foretaste of what identity management could become like in an AmI environment, when there will be many more systems, networks and services on offer. While there are some who believe that a single sign-on approach would reduce (somewhat) the complexity of interacting with a multiplicity of systems, others believe a decentralised approach reduces the risk that might arise from a massive failure or attack on a centralised system.

The snag with the growing complexity of computer communications systems, including those that will form the backbone of AmI networks, is that vulnerabilities increase with complexity. Experience has taught that systems — and, in particular, complex systems like networked information systems — can be secure, but only up to a point. There will always be residual vulnerabilities, always a degree of insecurity.[137]

From Scenario 3, second SWAMI report

Miles [*BBC reporter*]*: "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, 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."*

[136] Kent, Stephen T. and Lynette I. Millett (eds.), *Who Goes There?*, p. 63.
[137] Committee on Information Systems Trustworthiness, *Trust in Cyberspace*, National Research Council, National Academies Press, Washington, DC, 1999, p. 119.

Failures in identity management systems & authentication systems

If intelligence is embedded everywhere in an AmI world, there will be lots of people, companies, organisations collecting identity data. So questions will arise about their securing of our data. How well will supermarkets, or the corner grocery store, protect our identity data?

Security expert Bruce Schneier has said that it doesn't matter how well a system works, what matters is how it fails. No matter what their merits may be, if identity management, authentication and authorisation systems generate a large number of false positives, i.e., they authenticate or authorise someone to engage in some transaction when he shouldn't be permitted to do so, they will be regarded as failures.

It may be assumed that biometrics will ultimately reduce the number of false positives in view of the supposedly unique nature of each set of fingerprints, irises and other physiological features, but false positives are still possible. Sometimes these false positives are generated not by the technology but by those who wield the technology, as happened when the FBI became convinced, wrongly, that they had identified an Oregon lawyer, a Muslim convert, as a participant in the terrorist attack on Madrid trains in March 2004, on the basis of a single fingerprint which was a near match to one found in Madrid.

AmI networks generating false positives were depicted in Scenario 2 of the second SWAMI report.

"I guess I'll never feel comfortable with all these safety measures you have to endure when travelling: biometric ID verification, detectors for drugs and explosives, etc., especially if they reject you erroneously. 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! 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."

Problems like this *could* be reduced in an AmI world if the various AmI networks generate so much data about the individual that the individual is virtually unmistakeable. But if we arrive at that situation, it may also mean that there is a significantly greater amount of personal information floating around, so that the capture and analysis of such information reduces the very protection of privacy that identity management systems are supposed to support.

People do not take adequate care to protect their cyber identity(-ies)

Today cyber citizens often use the same password or ID over different websites and systems. The yellow bits of paper stuck on the side of computer screens with passwords written down undermine the point of having passwords. Unconsciously or not, most cyber citizens today do not take adequate care to protect their identity or identities. Some of the privacy enhancing technology schemes that are being considered for today's cyber world and that of the AmI world may help reduce this problem, but it's unlikely to go away. Human nature, being what it is, means that some people just will not take even the most basic of steps towards protecting themselves. From this optic, identity theft may have a salutary effect of being a good learning experience, but this is a bit like saying that walking

with your eyes closed across a busy street can be a good learning experience. In any event, once the theft has occurred, it may be as difficult or impossible to recover from as being run over by the number 9 bus.

Scenario 2 in the second SWAMI report makes reference to the failings in human nature…

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 [personal wrist communicator] *and HMDs* [health monitoring device] *early enough to avoid losing "our identity" like on our last trip…*

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.

Misplaced trust in security mechanisms

Any technology, including single sign-on, that requires you to relinquish control of your personal information should be regarded as a risk. Despite that risk, we may believe or we have been convinced that AmI PETs will protect us. In doing so, we may be trusting security mechanisms that don't warrant our trust. In some cases, particularly where we are required by law and/or by law enforcement authorities, we may be forced to rely on (to trust) the adequacy of security mechanisms, of others' privacy policies.

This is the situation in which we find ourselves with regard to national ID card schemes. Despite the criticisms voiced in the UK elsewhere about such schemes, Britons almost certainly, despite rearguard efforts by the House of Lords, will be forced to get a national ID card.

The national ID card has been criticised on many grounds, including cost. But in terms of security, Stella Rimington, a former director of MI5, has cast doubts on their efficacy as a security measure against terrorism. Security expert Bruce Schneier has said, "The potential privacy encroachments of an ID card system are far from minor. And the interruptions and delays caused by incessant ID checks could easily proliferate into a persistent traffic jam in office lobbies and airports and hospital waiting rooms and shopping malls. It won't make us more secure… No matter how unforgeable we make it, it will be forged… And even if we could guarantee that everyone who issued national ID cards couldn't be bribed, initial cardholder identity would be determined by other identity documents... all of which would be easier to forge… But the main problem with any ID system is that it requires the existence of a database… Such a database would be a kludge of existing databases, databases that are incompatible, full of erroneous data, and unreliable. As computer scientists, we do not know how to keep a database of this magnitude secure, whether from outside hackers or the thousands of insiders authorized to access it… A single national ID is an exceedingly valuable document, and accordingly there's greater incentive to forge it."[138]

In an AmI world, we may find an analogous situation, where identity management solutions are promoted by governments who expect us to take on trust that their solutions

[138] Schneier, Bruce, "National ID Cards", *Crypto-Gram Newsletter*, 15 Apr 2004. http://www.schneier.com/crypto-gram-back.html

are inherently safe and secure. Many of us may accept their logic and blindly put their trust in the proposed solution until hard experience teaches us otherwise.

3.4 IMPERFECT SECURITY

Security threats and vulnerabilities fall into two major groups: (1) malicious and (2) unanticipated system behaviour.

(1) Malicious system behaviour due to external attackers and insiders (authorised, but deceitful), which exploit internal system problems. Malicious system behaviour can be caused by criminals, insurance or trading companies (in order to increase their profit, they might want to acquire, e.g., information on drivers' driving behaviour or to modify user-defined filters in order to promote their own advertisements), by governmental organisations which fight against criminals by widespread surveillance, by employees and curious family members who want to benefit from spying.

Malicious system behaviour can be caused by viruses[139], worms[140], Trojans[141], phishing[142], denial of service attacks[143] or physical tampering.[144]

(2) Unanticipated system behaviour or failure due to insufficient design, e.g., internal complexity and lack of user-friendliness. The main reasons are:

- design problems, such as system use in circumstances not predicted by the system designer; programming errors; insufficient reliability or sources of critical components; poor scalability or performance of chosen communication protocols; inadequate range of wireless transmissions;
- an increase in the number of personal computers and lack of enthusiasm of their owners to invest significant efforts into secure system use (which is understandable: security is not the primary goal of most computer systems);
- lack of user-friendly security methods;
- incompatibility of system hardware components or software versions after a system upgrade (the diversity of possible software configurations and limited testing time make thorough testing of all configurations literally impossible);
- networking of personal devices and objects, including ad-hoc networking;
- economic reasons, such as uncertainty regarding costs of security holes.

---

[139] A virus is hidden, self-replicating software, that propagates by infecting – i.e., inserting a copy of itself into and becoming part of – another program. A virus cannot run by itself; it requires a host program to be activated

[140] A worm is software that can run independently, can propagate a complete working version of itself onto other hosts in a network, and may consume computer resources destructively

[141] A Trojan is software that appears to perform a useful or desirable function, but actually gains unauthorised access to system resources or tricks a user into executing other malicious logic

[142] Phishing means tricking the user into providing identity or banking data by asking the user to confirm his personal data on a fake website which pretends to be a legitimate site, and often looks exactly like a web page of, for example, a user's bank.

[143] Denial of service (DoS) is the prevention of authorised access to a system resource or the delaying of system operations and functions, e.g., the attacker sends huge number of extra messages to a target service provider

[144] Physical tampering means copying or changing data by physical manipulation of a device, e.g., replacing sensors in a sensor node so that they send wrong values

All of these threats can lead to:
- disruption of the primary operation of the technical system or even its destruction,
- violation of the physical integrity of the victim's home and property,
- endangering one's health and life,
- assaults against personal dignity and general well-being.

In the following sections, these threats and vulnerabilities are dealt with in greater detail.

3.4.1 Threats

Malware

Malware – spyware, adware, viruses, Trojans, worms, denial of service attacks – have been unfortunate features of daily life on the Internet and, lately, with advanced mobile phones. Often, malware is aimed at uncovering and exploiting personal and confidential data.

A recent survey by the National Cyber Security Alliance and America Online found that four of five computers connected to the Web have some type of spyware or adware installed on them, with or without the owner's knowledge. A UK survey found in 2004 that computer viruses, misuse of systems, fraud and theft had risen sharply over the previous two years. Two thirds of companies (68 per cent) suffered at least one such incident in the previous year, up from 44 per cent in the 2002 survey and just 24 per cent in 2000. Three quarters of the 1,000 businesses polled – 94 per cent of the larger companies – had a security incident in the last year. The average UK business now has roughly one security incident a month and larger ones around one a week. Security breaches frequently left systems inoperable.[145] And the proliferation of malware continues to get worse: spyware reportedly trebled in 2005 over the previous year.[146]

Most computer users acquire spyware and adware simply by browsing certain Web sites, or agreeing to install games or software programs that come bundled with spyware and adware. Computer users may or may not understand what they are consenting to when they click "OK" to the lengthy, legalistic disclosures that accompany games or videos. But those notices are legal contracts that essentially absolve the adware companies from any liability associated with the use or misuse of their programs.[147]

From Scenario 1, second SWAMI report

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. Companies are paying a lot of money for personal and group profiles. This phenomenon is known as "data laundering". Similar to money laundering,

[145] Leyden, John, "Hackers cost UK.biz billions", *The Register*, 28 April 2004. http://www.theregister.co.uk/2004/04/28/dti_security_survey/
[146] Kelly, Lisa, "Spyware attacks triple in 2005", *Computing*, 12 Jun 2006 http://www.vnunet.com/computing/news/2158112/spyware-attacks-triple-2005. See also Krebs, Brian, "Microsoft Releases Windows Malware Stats", *The Washington Post*, 12 June 2006 http://blog.washingtonpost.com/securityfix/2006/06/microsoft_releases_malware_sta.html
[147] Krebs, Brian, "Invasion of the Computer Snatchers", *The Washington Post*, 19 Feb 2006

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.

Once installed on a PC, adware serves up pop-up advertisements and mines data about the user's online browsing habits. The computer worm that powers a botnet also gathers sensitive data from the victim's machine, including passwords, e-mail addresses, Social Security numbers and credit card data. The spyware and adware problem is pervasive and growing.[148]

We might assume that those who install adware, spyware and other malware on our machines do so with malicious intent. They are the bad guys, the ones in the black hats, but we've discovered that even hitherto respected big corporations have resorted to similar tactics.

In an attempt to minimise the proliferation of unauthorised copies, copyright owners are employing digital rights management (DRM) technologies to control access to intellectual property. But DRM technologies may pose threats to privacy through collection of information about individuals' digital consumption and preferences. Arguably, such DRM technologies are engaged in a form of surveillance, i.e., what we watch, listen to, read or use, when and for how long. The data they gather can all be added to our profiles for more targeted marketing, greater personalisation of services, spamming and government oversight. DRM technologies can be embedded in video and audio products as well as other software packages. They can be imprinted on supposedly "blank" DVDs or CDs, so that when we copy something while connected to the Internet, the DRM technology can surreptitiously report back to the copyright holder whether we have made a legal copy or not.

Last November, Sony was found to be shipping copy-restricted compact discs that planted rootkit software on the computers that played them. The rootkit technology offered a hiding place for malicious software and attackers, which were quick to exploit it.[149]

After the rootkit technology was uncovered on Sony's CDs, the company faced heavy criticism and lawsuits. It recalled the discs, stopped production and has agreed to offer compensation for buyers of the CDs that contain the rootkit.

Since the Sony case, other companies have been accused of shipping products with rootkit-type behaviour. Symantec last month released an update to its popular Norton SystemWorks to fix a security problem that could be abused by cyber criminals to hide malicious software.[150] Microsoft has admitted that it neglected to tell users that its Windows Genuine Advantage (WGA) was phoning its Redmond offices every day.[151]

---

[148] Krebs, Brian, "Invasion of the Computer Snatchers", *The Washington Post*, 19 Feb 2006

[149] Wikipedia defines rootkit as a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge. Rootkits are known to exist for a variety of operating systems such as Linux, Solaris and versions of Microsoft Windows. A computer with a rootkit on it is called a rooted computer.

[150] Evers, Joris, "America 'must consider banning rootkits'", CNET News.com, 17 Feb 2006.

[151] Oates, John, "Microsoft product phones home every day", *The Register*, 8 Jun 2006 http://www.channelregister.co.uk/2006/06/08/ms_wga_phones_home/

It should be no surprise that government agencies have installed bits of software on users' machines. Recently, the US National Security Agency was found to be placing cookies on the computers of visitors to its website in order to track their Web surfing activity despite a federal ban on doing so. NSA acknowledged yesterday that they had made a mistake and stopped doing so after a privacy activist complained and after inquiries by the Associated Press.[152]

Can we expect a cleaner future in a world of ambient intelligence? Or will new forms of malware be created in order to exploit an Internet of things and fourth generation mobile phones? Clearly, we should assume that malware will be a part of our future just as it is daily phenomenon today. Already there are concerns about threats to Voice over Internet Protocol (VoIP). We should assume that our AmI environment will be under attack not only by criminals, but also by industry and government.

Data mining and networking

Growing opportunities to make money via computers inevitably increases the number of attempts to acquire personal data. Such opportunities include, first, commercial structures: it helps to know an individual's personal financial situation and personal preferences in order to present him or her an attractive offer. Second, insurance companies might search for personal data in order to impose higher insurance fees on those users whose profiles suggest they are higher risks (e.g., users who often drive at night or who engage in dangerous sports such as skydiving). Both categories of interested organisations might provide financial support to developers of spyware.

Third, increased opportunities to perform a crime remotely via networks (such as phishing or remote control of somebody else's personal belongings) also threaten security.

Surveillance

Law enforcement authorities and intelligence agencies' interest in surveillance in order to increase the security of society as a whole (on the assumption that total surveillance can help to decrease number of terrorist acts) might hinder development of anti-spyware tools if they do not receive adequate financial support, or limit usage of such tools by general public. The main problem with security is that security is not a primary goal of computer usage; and security measures are often neglected if they are not user-friendly. Thus, security of personal devices depends on how much governments support research, development and distribution of user-friendly security measures. Governments have the power to increase taxation of anti-spyware products and wiretapping detectors (or even to make them illegal), or to make them free of charge.

Inadequate profiling

Inadequate profiling may not seem like a security threat at first glance, at least not in the traditional understanding of security flaws as a malfunctioning of or as attacks on computers. However, nowadays the term "security" is often being used in a sense related to the safety of individuals, groups or societies. For the safety of users, inadequate profiling

[152] Associated Press, "Spy Agency Removes Illegal Tracking Files", published in *The New York Times*, 29 Dec 2005. http://www.nytimes.com/2005/12/29/national/29cookies.html

can present a threat if it forces users to attempt to fit into right profile or if it generates false positives. For example, if insurance companies impose higher fees on users whose lifestyle they consider "insecure" (e.g., if their food consumption, driving behaviour or recreational activity do not fit their standards), the users are left with the choice of paying more or changing their behaviour according to the wishes of the insurance companies; and this forced behaviour change might be dangerous for their health and life. For example, refusal from usual food might cause allergy or lack of microelements.

The main question is what is a standard and who is defining it.

3.4.2 Vulnerabilities

Increase in personal use of computers and other devices with limited resources

In earlier days, computers were not really personal: people were mainly using computers owned by their employers, who took care of computer security, timely updates of hardware and anti-virus software, compatibility of installed applications and so on. In today's world, computers have become increasingly personal; modern mobile phones are themselves fairly powerful personal computers. Consequently, the burden of taking care of security of personal computers has shifted towards individual users.

This burden can be a hassle even for those who only have to care about the security of their own desktop computers; the situation becomes worse in the case of mobile devices with limited capabilities. Mobile devices have already replaced desktops in many tasks, and this trend will increase in the AmI future. This increases threats to security because running sophisticated encryption algorithms and communication protocols and multi-tasking are difficult for mobile devices. Additionally, limited battery life carries a danger that the device becomes useless unexpectedly; the small screen size of mobile devices carries a danger that users will miss important information due to an unwillingness to scroll down, and so on.

Lack of user-friendly security measures

Despite the fact that users must take care of their own security, the security of personal devices has not significantly improved compared to the early days of desktop computers: the main means of user authentication in mobile phones is still a PIN code, and user authentication happens only when the phone is switched on. Besides, proper configuration of security settings requires a certain education (which most users don't have), while updates of software require significant explicit user effort. Even software updates on personal desktops are not user-friendly; the need to restart the computer after every update is a hassle.

Consequently, it is not reasonable to expect that all users will take care of timely updates of their anti-virus software or authenticate themselves to their devices frequently enough, and this might be very dangerous.

Networking of personal devices and objects

The vision of AmI is associated with everything communicating with everything: objects, organisations and personal devices constantly exchange messages. This endangers security

significantly because one malicious network node can create problems for surrounding nodes if it constantly broadcasts messages and requires replies. A malicious node can spread viruses or distribute false data. Even if other networking devices have good anti-virus protection and don't get infected by this malicious node; and even if they are able to conclude that the received data are not trustworthy, part of their limited communication and computational capabilities and battery life are wasted anyway.

Additional security problem arise from the inflexible communication range of devices: radio signals from devices and objects located in one home or in one car can easily penetrate walls, so that thieves could detect whether a flat is empty or not, and break into one that is. Another problem is created by the sheer increase of radio communications, which can hinder device operation in some cases (see section 3.4.1 for examples).

Increase in diversity of hardware and software

Since more and more versions of hardware and software appear in the market, the problem of compatibility between different hardware components connected together and between different versions of software (running on the same device or during attempts to communicate between different devices) becomes critical. Moreover, that incompatibility can be invisible to the user in the sense that devices still function and communicate, but more slowly or with errors: e.g., incomplete compatibility in communication protocols can lead to distortion of transmitted data without the user's noticing it. Incompatibilities between new anti-virus software and old operational systems can lead to security holes and so on.

Uncertainties about costs of software imperfection and improper security

Security has a cost. As long as market requirements or legal regulations do not force manufacturers to provide products with user-friendly security included, and as long as costs for security problems caused by insecure products are somewhat indeterminate (who knows how to estimate the cost of manually deleting 100 spam e-mails, or recovering from identity theft?), the AmI world will face serious security problems. It is impossible to predict all possible configurations of components that users might install on or connect to their devices and increasing competition between companies producing software and hardware increases the risk that the testing of devices and software may be insufficient to cope with potential security vulnerabilities. In addition, it is impossible to predict all possible configurations of components that users might install on or connect to their devices.

Growing complexity of systems and design problems

The growing complexity of systems increases both the risk of unpredictable system behaviour and the risk of malicious attacks due to security holes caused by the interaction of components. Interactions between operational systems, ant-virus software and customer applications can hinder the functionality of anti-virus software and increase the risk that virus attacks will succeed. They can also slow down customer applications. The complexity of customer applications can cause unpredictable behaviour if applications are used in situations or ways not predicted by their designers (and designers will not be able to predict everything). Further, the reliability and performance of critical components may be insufficient for the ways in which the components are ultimately used.

3.4.3 Disruptions to the primary operation of a technical system

The primary operation of a technical system can be disrupted in many ways. For example, in a health care emergency, it may be necessary to connect a patient's personal device to the hospital network in order to acquire the patient's health care history. In order to interoperate with the hospital's emergency network, the patient's personal device may need to be reconfigured, which in turn could disrupt the operation of personal device or of the emergency network.

Example from Scenario 2:
What I did not know was that some passengers were using HMDs [health monitoring devices] 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.

If the patient's personal device is contaminated with viruses, they may be transferred to the hospital's AmI system together with the patient's data or to another personal device.

Example from Scenario 1:
Maruja receives the message from her daughter [with the attractive offer to buy a game] just before a business meeting starts. She looks at the message in a hurry [and clicks on the link]. Both Maruja and her daughter are not aware that the website with the attractive offer contains a powerful spyware program that looks for personal data and personal preferences, so that they can be targeted with personalised advertising.

Another common problem is that gaming applications often consume a lot of system resources and often suggest that the user upgrade to a new version or plug in a new piece of hardware. This upgrade may cause compatibility problems, harming other functionalities of a personal device. Similarly, an upgrade of a factory automation system may decrease the system's performance because of incompatibilities between different components.

Another example of disruption occurs when a personal device with limited resources becomes too busy processing a large number of incoming messages (e.g., sorting advertisements according to the owner's preferences). Consequently, managing other tasks of the personal device (e.g., notifying the user about incoming e-mails from friends) may slow down significantly. Proper prioritising of the device's tasks would help, but setting priorities may be a burden for the user.

Example from Scenario 1:
Maruja leaves the office for a lunch break. She decided to buy a take-away sandwich and walks towards the park. She is receiving almost continuously [advertising] messages on the flexible screen on her sleeve... 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. Later, she finds out that her boss phoned twice. She also missed a proximity message that a good friend was sitting in a nearby pub.

Similarly, if too many wireless messages are transmitted in the environment, some smart object with limited resources (e.g., keys with an embedded hardware module which should help us to find them if they are lost) may miss our only important query and thus the keys remain invisible to us. Even worse, operation of pacemakers or implants may be disrupted by radio inference from nearby intensive wireless communications.

Deliberate attacks can disrupt or even destroy the primary operation of a technical system. Many, if not most networks are vulnerable to denial-of-service attacks. Such attacks can completely ruin wireless mobile devices if the battery discharges. Besides, security gaps may allow software code to be modified or replaced so that the system fails to perform as intended by its system designers. Tough competition might stimulate the development of viruses that change user preferences in such a way that only certain product brands pass the filters. Some miscreants might be so irritated by traffic control systems that they might create malicious code that change traffic priorities so that they can get access to the fastest lanes and thereby mess up the whole system. One can envisage many similar possibilities.

Example from Scenario 2:
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 had hacked the system for getting right of way at any intersection. 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.

3.4.4 Threats to and vulnerabilities in home and property

Home and property may be threatened by malicious actions: criminals may gain improper access to home networks allowing them to cause arson or gas leakages remotely, to check and steal valuables from the home or car. M-commerce applications and phishing (cheating users into providing credit card or banking information to fake websites) can lead to identity theft and financial loss. Criminals may engage in blackmailing: if they can demonstrate that they control home systems, they can put severe pressure on residents.

Example from Scenario 1:
Paul is receiving multiple messages on his PWC [Personal Wrist Communicator] the moment he leaves his boss's office ... There is one message that immediately attracts his attention. "If you want your house systems to work again, click on the following link…"

Customer profiling can effectively contribute to the disinformation of users. For example, if a shop owner's system knows that a client is wealthy, it might suggest only expensive items to that client, so that the client is not aware of cheaper options, either in the same shop or that of a competitor.

The physical integrity of the home and property is vulnerable to internal system problems in the following ways: With the growing dependency on AmI systems, users naturally will not care as much as nowadays to switch off the stove, to adjust heating, to close windows, to check that their wallet is still in their pocket and so on. Consequently, system failure in any of these AmI applications may lead to dire consequences: the stove overheats and

causes a fire; a thunderstorm destroys valuable items because the windows were not shut; unnecessary extra payments are made for heating or water consumption; wallets are to forgotten and so on.

3.4.5 Threats to and vulnerabilities in health and life

Threats to health and life can be caused by malicious actions such as the following: intentional disruption of life-critical application (e.g., denial of service attack on a network of health monitoring or traffic control devices) can allow remote homicide. Another way to arrange a murder remotely would be to alter a health-monitoring device, for example, to replace sensors so that they send values indicating good personal health even if the person has a heart attack. Leakage of personal location data can facilitate kidnapping. Desire to spoof biometric access control system can prompt criminals to cut off fingers of authorised persons. Humiliation of a person (e.g., by disclosure of personal secrets) could lead to suicide.

Our health and lives are vulnerable to failures in all sorts of computerised applications. For example, any failure in health monitoring or health care applications (error in diagnosis, failure to transfer personal data at the right moment, failure to remind patients to take medicine, disturbances to pacemakers due to radio interference) may endanger personal health and life. Similarly, any failure in traffic control or warnings about approaching cars may lead to accidents. A failure to switch off the gas may put health and life at risk too. Failures in industrial systems may also cause dangerous accidents. Thus, security measures should include critical infrastructure protection. Critical infrastructures are complex and highly interdependent systems that provide the services required in daily life. Electric power, water, transportation and telecommunications are just a few of the critical infrastructures on which we depend. With the increasing dependence of these systems on computer networks, security of critical infrastructure has already become a major issue.

Additionally, personal health is vulnerable to a too-high density of wireless communications and different kinds of ambient radiation

Example from Scenario 2:
But something really tragic occurred with Monika Klein, a nice 84-year 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 feeling quite okay, 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 practise the simplest diagnostic methods. Otherwise, they would have noticed that Mrs Klein had internal bleeding. I heard that when they took her to the hospital as one of the last, she suddenly lost consciousness and passed away before the ambulance reached the hospital.

3.4.6 Threats to and vulnerabilities in personal dignity and general annoyance

Our personal dignity is susceptible to malicious actions caused by viruses, spamming, denial of service and surveillance by government, insurance companies, employers, family members, neighbours, etc. Such threats can be realised by changing program code or

reconfiguring a system in such a way that the user does not know how to get back to normal system operation. Identity theft and compromised personal data could cause personal stress.

Example from Scenario 3:
We heard about one case involving a senior civil servant... 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.

Our personal dignity is vulnerable to numerous internal system problems, including: lack of system intelligence such as the inability to distinguish between task-related information and other data, possibly leading to accidental disclosure of sensitive data; giving reminders too frequently; insufficiently high performance of algorithms (poor encryption or slow decryption or errors in person recognition); insufficiently intelligent anti-virus and anti-spamming software; losses of important data due to system complexity or viruses. While such a vulnerability might not lead to severe consequences like the previous ones, it is likely to be one of the most frequently realised.

The following example from Scenario 1 shows how the lack of system intelligence (inability to recognise that the current user context is not suitable for displaying sex-related products) leads to the personal frustration.

Example from Scenario 1:
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.

3.5 UNDERMINING TRUST

One of the most important inhibitors to public acceptance of the Internet for human interactions (commercial or otherwise) has been the lack of trust in the underlying cyber infrastructure and in other people whom we meet through that infrastructure. Incidents of massive identity theft from otherwise internationally trusted financial institutions, the never-ending resourcefulness of malicious hackers, intruders and spammers, have increased the apprehension and uneasiness of the general public vis-à-vis the Internet and the Web – and there is strong evidence that this will apply to an even greater extent to ambient intelligence services in the future.

It is a challenge to change this climate not only at the level of interactions among human agents (commercial or otherwise) through the use of the cyber infrastructure, but also among human and software agents. This is a grand challenge, since the "mechanics of trust" may vary drastically between different cultures. Moreover, there are trade-offs between trust and privacy, trust and security, and trust between commercial competitors that are not easily brought to a balance.

In the following, threats to and vulnerabilities in trust will be discussed with regard to four areas: inadequate profiling, loss of control, service refusal and discrimination, and victimisation. These areas are closely interrelated. For instance, poor profiling is a problem because the promised customisation might be deficient and, at the same, because it represents a precondition for certain denials of services. Thus, distinctions between the four areas have been introduced for analytical purposes. Moreover, as the concept of trust is multi-dimensional, largely intangible and encompasses interdependent relationships, problems primarily related to privacy, identity, security and the digital divide are relevant for the issue of trust as well.

3.5.1 Inadequate profiling

As the AmI vision is geared towards a user-driven approach, one of the key means of meeting the users' individual needs is personalisation. In order to be able to deliver customised services, user-specific profiles need to be created. Profiling in an AmI environment consists of constantly collecting and processing a broad range of data from numerous sources that are related to a user's identity, his/her activities, characteristics and preferences in specific environments. Based on constructed profiles, AmI systems able to respond to the users' needs – or at least what is assumed to be their needs inferred from the interpretation of the collected information. Problems of inadequate profiling can occur in two main situations: attribution conflicts involving numerous users and misinterpretation of users' needs.

Multiple users

In the case of incorrect attribution, two or more users are concurrently present in an AmI environment. The users' profiles, actions and preferences may not necessarily be congruent.[153] If profiles are completely or even partially incompatible, conflicts over shared services and resources might occur. If these conflicts are not resolved adequately, user acceptance is at stake. A possible solution is to average out the disputed profile parameters. However, in many areas of daily life – for example, where users have different musical preferences – such simple mathematical remedies are not feasible.

Misinterpretation of needs and inadequate expression of preferences

The quality of a personal profile depends both on the scope and depth of the input data as well as on the adequacy of the data processing routines. However, even if service providers decide to invest sufficient resources into the continuous monitoring by numerous sensors and the development of "intelligent" software in order to improve the performance of an AmI system, the profiles developed from the collected data can merely represent – at best – constructed approximations of the actual user preferences. Information collected by AmI sensors is mainly based on observed patterns of behaviour. Thus, just as in the case of empirical social research, profiling can merely capture a simplified extract of a complex reality; moreover, the data tend to be distorted by artefacts. In short, linking observable behaviour to an individual's intentions is highly problematic and prone to misleading interpretations – a challenge, of course, faced by every developer of an "intelligent" system.

[153] Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick, "Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence", FIDIS Deliverable D7.3, 2005, p. 12.

The most common approach to ease the problem is to supplement the profiling process by requesting direct input from the user. However, this is not only at odds with one of the envisioned key characteristics of AmI – namely the disappearance of user interfaces – it also entails other considerable trade-offs. The predefined choices can either be very limited, hence constraining users' options profoundly. Or, if the opposite strategy is implemented and very detailed choices are offered, the user is burdened with time consuming and perhaps annoying adjustment and programming procedures. Moreover, this method can only be successful to the extent that the user is, firstly, cognisant of her/his preferences and, secondly, fully able to identify and articulate his/her needs in the required form. Most dimensions of human self-expression include implicit, intangible, subtle and fuzzy forms, making it – at least for the time being – impossible to reconstruct them adequately. In addition, if individual preferences with regard to a specific application or situation tend to change frequently and dynamically, the expediency of user-supported profiling is significantly reduced.

These considerations on profiling are not intended to support the conclusion that profiling is to be dismissed per se. Instead, a better understanding of the innate limits to the construction of user profiles should entail a heightened awareness of the necessity to implement adequate provisions that help to reduce undesirable side-effects. This could, for instance, be achieved by system designs that always enable users to easily overrule decisions made by an AmI system.[154]

Example from Scenario 1:

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.[155] *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.*

"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 had 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 had a sandwich, because she paid for it by cash.

3.5.2 Loss of control

The problems associated with loss of control can arise from (1) simple annoyances in day-to-day interactions with AmI, (2) uneasiness caused by the lack of transparency of systems operating in the background, (3) unpleasant or even frightening experiences if one is confronted with unexpected system behaviour, and (4) serious intimidations caused by

[154] Spiekermann, S., and F. Pallas, "Technology Paternalism – Wider Implications of Ubiquitous Computing", *Poiesis & Praxis*, Vol. 4, no. 1, 2006, pp. 6-18.
[155] Espiner, T., "Philips unfurls prototype flexible display", *ZDNet UK*, 2 Sept 2005. http://news.zdnet.co.uk/hardware/emergingtech/ 0,39020357,39216111,00.htm

malicious exploitation of technical vulnerabilities. In the first case, the system design did not consider sufficient possibilities for users' control over the system. Failures of this kind originate in inadequate incorporation of user preferences and behavioural patterns in system design. Once more, the general problems with regard to adequate profiling establish natural limits to this remedy. In the second case, the very embeddedness and cloaked nature of many AmI services is accompanied by a lack of transparency. In the third case, the combination of technology dependency and a lack of understanding evoke stress and anger if the system does not behave as expected. And in the fourth case, security measures have been circumvented.

Technology paternalism

One of the main rationales for creating and implementing AmI systems is to assist in the management of complex processes, which previously had to be accomplished by the user. Thus, the declared objective of the AmI system is to take a certain burden – mostly standardised tasks with frequent repetitions – away from the individual in order to raise the level of convenience, security and/or efficiency. The commonly envisioned application areas of AmI systems are manifold and well known, including the management of environmental parameters such as room temperature, lighting, etc., according to individual preferences; the management of communications according to predefined rules and/or based on machine-learning;[156] and implementing security provisions in mobility situations restricting certain behaviour or informing the user in case of a potential danger.

Technology paternalism[157] arises in those instances in which machines decide autonomously and uncontrolled on behalf and in the supposedly best interest of a user. Technology effectively infringes upon individual liberty if no easy-to-use and convenient override options are available and the user does not want to comply with the settings of an AmI system – for whatever reason. The possible drawbacks from technology paternalism can range from constant irritations to fundamental distrust in AmI, possibly leading to the deliberate decision to avoid AmI systems as far as possible.

Example from Scenario 4:

"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…"

Lack of transparency

As has been pointed out, one of the central features of many existing and envisioned AmI applications is their ability to operate in the background, largely unnoticed by the user. While this defining characteristic doubtlessly has its merits in terms of usability, convenience and efficiency, it may have adverse effects on users' trust in and acceptance of AmI services. Because users know that AmI systems can operate invisibly,

[156] Cf. the above-mentioned difficulties in constructing adequate profiles.
[157] For a detailed discussion of the concept, see Spiekermann, S. and F. Pallas, "Technology Paternalism – Wider Implications of Ubiquitous Computing", *Poiesis & Praxis*, Vol. 4, no. 1, 2006, pp. 6-18.

autonomously and unperceived, concerns about system control, the possibly hidden agendas of system operators, and secondary use of collected data may arise. In fact, a recent consumer study dealing with acceptance of RFIDs confirmed that users tend to consider themselves as powerless and helpless and feel that they are being left without real choices due to the loss of control in certain AmI environments.[158]

In conventional technology acceptance models, the willingness to use a technology is typically dependent upon its perceived *usefulness* and its *ease of use*.[159] As many AmI services are envisioned to function autonomously in the background, unwillingness and reluctance to use these systems can hardly be ascribed to complicated usage requirements.[160] In fact, other acceptance criteria need to be added to the equation. Due to the absence of interfaces and direct human-machine interaction opportunities in AmI environments, it stands to reason that (dis)trust plays an even more important function with regard to user acceptance of AmI than is the case for most other technologies. An approach to alleviate concerns about latent operations and data misuse, thus reducing distrust, is to enhance transparency by effectively informing users about system procedures, purposes and responsibilities.

Unpredictable or unexpected system behaviour

The AmI vision promises a natural, intuitive and, therefore, unobtrusive way of human-technology interaction. If such a smooth co-operation cannot be attained, there is a risk that ambient intelligence will cause stress and distrust and, as a consequence, the technology will not generate the acceptance necessary to realise the (societal) benefits it promises.

Due to the technology's complexity or the different conception that program developers and users have of the proper use of information systems, users may conclude that they cannot rely on the AmI technology as expected. This is especially true for distributed systems whose behaviour is particularly difficult to predict. The possibilities of formal verification, which would ensure that unwanted system states couldn't occur, are limited in this case.

This is a problem especially for those users who are not familiar with information technology. These users often blame themselves if they do not attain the desired goal and are often too reluctant for a second try because they are afraid of damaging something. Only those groups that are always open-minded towards new technologies will adopt AmI and incorporate it into their daily life in the short term.

As the dependency on such systems increases, the potential harm, which could result from a misjudgement of system behaviour, also rises. Where more is at stake than the result of a few hours' work (as is the case with normal computer use today), the distrust of users will increase accordingly.

---

[158] Spiekermann, S., and M. Rothensee, *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing*, Institut für Wirtschaftsinformatik, Humbold-Universität zu Berlin, 2005, pp. 7-9. http://interval.hu-berlin.de/downloads/rfid/neuste%20forschungsergebnisse/SocioPsychofak.pdf.

[159] Cf. Venkatesh, V., "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model", *Information Systems Research*, 11(4), 2000, pp. 342-365.

[160] Spiekermann, S., and M. Rothensee, *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing*, Institut für Wirtschaftsinformatik, Humbold-Universität zu Berlin, 2005, p. 5. http://interval.hu-berlin.de/downloads/rfid/neuste%20forschungsergebnisse/SocioPsychofak.pdf .

Example from Scenario 2:

"Heike's attempts to call her parents are not successful. As she learned later that day, in an emergency situation, the HMDs [Health Monitoring Devices] *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."*

Hijacking an AmI system

In the case of a hijacked AmI system, the user's loss of control is not caused by default system settings. Instead, the situation clearly depicts a deviation from normal procedures due to malicious or criminal interference. Once hackers and attackers gain full or even partial control over the AmI system, they might be able to re-adjust personalised settings and extract sensitive information stored in databases in order to use them illegally.

Example from Scenario 1:

Paul receives multiple messages on his PWC the moment he leaves his boss's office.[161] *He had all incoming communications on hold from the moment he entered her office. This is a company default setting. There is one message that immediately attracts his attention. "If you want your house systems to work again, click on the following link…" "What? I'm being blackmailed! So that's why I couldn't get access to my home systems, nor could the local security agent. That's why I got the intruder message," he thinks, slightly reassured, since that probably means that his children at home are OK.*

3.5.3 Denial of service and discrimination in case of inadequate profiles

Other than in the case of inadequate profiling in which the deficiencies are caused by discrepancies between individual preferences and poorly constructed profiles (see above), denial of services and incidents of discrimination originate in procedural rules imposed by service providers – either in their own right or in compliance with regulations established by public authorities. In the first case, the individual preferences are the central point of reference for the AmI system; in the latter case, specified profile characteristics have to be met by the individual if he or she desires access to certain services or privileges. Furthermore, a closer look into the general problem of service denials reveals that a user might not only be turned down because his/her profile does not match the required criteria (e.g., income, age, health record or other aspects of the personal data history). It is conceivable that an individual's deliberate decision not to make available certain elements of personal data will result in exclusion. This raises the two issues of proportionality and of the possibilities of opting out without experiencing undue restraints. Furthermore, the sophisticated issues to what degree information disclosure is actually necessary in order to achieve certain objectives (smoothly functioning services, civil security, etc.), which types

[161] Alahuhta, P., M. Jurvansuu and H. Pentikäinen, *Roadmap for Network Technologies and Services*, Tekes, Helsinki, 2004. http://www.tekes.fi/julkaisut/Roadmap.pdf

of information service providers should not be allowed to ask for and which additional data sources might be used are touched upon.

Situations in which discriminatory refusals of services can take place are characterised by asymmetric relationships in which one party is obliged to comply with standards defined by the other party – though this will be hard to distinguish from the freedom of contract in individual cases. Two main realms of discriminatory practices due to allegedly inadequate profiles can be distinguished: concerns regarding civil security and practices mainly driven by commercial interests.

- **Civil security:** Based on security concerns, users are requested to provide personal information as a prerequisite to gain access. In most cases, certain requirements have been established by public authorities, and private companies (e.g., transport services, airports, etc.) are obliged to implement these regulations. However, in cases of service denial, it is not necessarily clear to the user on which grounds the measure was imposed. Apart from the possibility of a technical error (e.g., faulty database), it is difficult to discern whether the refusal is based on public regulations or the service provider's own rationale – which draws attention to the second type of discriminatory practice. Other reasons for the refusal of services can either be inadequate interoperability of information systems or, in the case of individuals from less developed regions, the absence of personal profile data.

Example from Scenario 2:

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! 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.

- **Profit interests:** Apart from pure security motives, market and profit considerations can be at the heart of access rules. For instance, customers might be coerced into making available sensitive personal data if they wish to enjoy certain privileges or services (e.g., special insurance premiums, rebates, etc.). Moreover, if a customer deliberatively decides not to comply for legitimate reasons, a service provider might respond by limiting its own liability. Apart from any legal considerations, it seems quite obvious that users who have experienced being deprived of real consumer choices will not develop pronounced trust in AmI applications.

Example from Scenario 2:
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.

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

3.5.4 Victimisation

Due to faulty profiling, an innocent individual might erroneously be identified as a criminal, a potential security threat or even a terrorist.[162] Apart from technical problems, the likelihood of mistakenly suspecting a person increases if the objectives of security needs and personal privacy rights are not balanced adequately. Moreover, incomplete and/or de-contextualised profile information may also contribute to the victimisation of citizens.

Example from Scenario 1:

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

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

3.6 THE ENDURING DIGITAL DIVIDE

A broad range of threats and vulnerabilities in AmI space relate to the digital divide issue. Amongst the most important ones are different aspects of dependency, exclusion and discrimination.

3.6.1 Dependency

For the purpose of this report, two types of dependency are identified: system and user dependency. **Technological dependency** refers to the fact that the proper functioning of a technology or a technological system such as AmI depends on the availability of other technologies of the same or even a previous generation. Due to the ubiquity of AmI, the likelihood of technological dependency will be amplified.

User dependency relates to a user's severe irritation, frustration or even panic if a certain technological function or service is temporarily not accessible, not available or does not function properly. In its extreme form, user dependency can display symptoms similar to those of psychological addictions or obsessions.

In the paragraphs that follow, certain vulnerabilities and/or threats regarding the creation of digital divide are presented in detail, for each type of dependency. Nevertheless, the issues that stem from user dependency are not directly related to digital divide but rather to social

[162] Exactly this situation already occurs today. See, for example, Summers, Deborah, "Bureau admits innocents branded criminals", *The Herald* [Scotland], 22 May 2006: "The Home Office was plunged into yet more controversy yesterday as it emerged nearly 1500 innocent people had been branded criminals because of errors by its Criminal Records Bureau." http://www.theherald.co.uk/politics/62460.html

disturbances, generated by an individual's unusual (other than his/her usual) behaviour. However, given the study's focus, i.e., safeguards in the world of ambient intelligence, it has been considered important to identify and present them here.

Technological dependency: insufficient interoperability

This vulnerability is caused by technological dependency and has two main aspects: spatial and temporal. The spatial aspect concerns the lack of interoperability between geographical entities. In order for AmI to function across borders, different regions and countries need to use technologies that interoperate. Further harmonisation of standards with varying degrees of geographical scope will be needed (e.g., EU, international). Some countries, however, will not be able to afford to fully comply with the standards created in developed countries. Solutions to overcome the potential divides based on insufficient interoperability need to be envisaged.

Example from Scenario 2:
What I did not know was that some passengers were using HMDs [health monitoring devices] *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.*

Another example from Scenario 2:
A woman died because her health monitoring system was not compatible with the local (network health) system. Her injury was not detected

The temporal aspect refers to the lack of interoperability between different generations of tools and devices. This vulnerability may lead to the categorisation and, consequently, the discrimination of users based on socio-economic status or even because of conflicts of interests and preferences (see example from Scenario 4).

Example from Scenario 4:
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.

High update and maintenance costs

On the one hand, the drive towards cost-savings could give a boost to the implementation of AmI, but on the other hand, maintenance and updating could be much more costly than initially expected. Therefore, high costs may lead to the widening of the digital divide within societies, where some people would be able to afford costly maintenance and some would not. It could also become apparent between different countries or nations, since the developed ones could afford these costs whereas the developing or under-developed could not.

Example from Scenario 2 (Social digital divide, i.e., among people within the same society):
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, …

Example from Scenario 4 (Global digital divide, i.e., between nations):
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.

User dependency: Systems take control

This variant of user dependency is caused by a temporary or even total loss of control over an AmI application (due to inadequate system design, for instance). As a consequence, the user might not receive the expected service from the application.

Example from Scenario 1:
"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.

"AmI technosis"

The disruption of social behaviour might be caused by a user's over-reliance and dependency on new means of communication made possible by AmI technologies. In this sense, the user may be or feel excluded.

Example from Scenario 1:
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

Stress

Severe dependency on technologies may lead to stress. If the technology we have fully integrated into day-to-day routines is not accessible (even temporarily), we will not be able to perform in the usual way. Stress may result from uncertainty as to whether it is possible to re-establish a previous functional state.

Example from Scenario 1:
Paul receives an alarm signal on his Personal Wrist Communicator (PWC). There is an intruder in the house. "How is that possible?" he asks himself. He knows that his son Ricardo is home. He had invited some friends to play a new virtual reality game (for which Ricardo has a licence) from the entertainment centre downstairs. Paul checks the home surveillance system remotely but only gets a still image from 30 minutes ago. There is no live image available from the front and back door cameras, nor is Paul able to play

back who has passed in front of the doors today. Ricardo does not answer his calls. "What's happening? Where is he?"

Unsafe usage (due to lack of rules)

The ubiquitous aspect of AmI technology enables usage on the move, i.e., allowing individuals to use it nearly everywhere, which may sometimes lead to incorrect or unsafe use, either by mistake or even on purpose, with consequences that might not be easily anticipated.

Example from Scenario 4:
Concert mode allows everyone in the venue to interconnect, but it also gives event organisers a direct channel of communication in case of emergency. -- Last night, not everyone made the switch to 'Concert' mode. … 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.

3.6.2 Exclusion and discrimination

As stated before, digital divide is often referred to as "information exclusion", where people are excluded from but also by information. In this sense, exclusion and discrimination regarding new technologies are two important aspects of digital divide[163], in the context of which certain threats and vulnerabilities may arise, as referenced in the following paragraphs.

Unequal access

AmI technology has the potential – due to its foreseen user friendliness and intuitive aspects – to bridge some aspects of the current digital divide. On the other hand, AmI technology could also amplify other aspects of unequal access and use. This threat has technical as well as social and organisational dimensions. There are no guarantees that ambient intelligence services will become public utilities to the benefit of all. There will still be many people with limited or no access to more sophisticated AmI applications, and thus they will be unable to receive any of the envisioned value-added services and the expected benefits of the AmI environment. This is also the case between developing and developed countries or nations.

Example from Scenario 3:
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.

Stigmatisation / profiling

Because many AmI technologies and devices will need profiling data in order to provide users with the expected and suitable services, profiling data will proliferate within the AmI

[163] The aspects, dimensions and determinants of digital divide are more thoroughly presented in section *2.5 Digital Divide*.

networks. The misuse of profiling data by companies or other organizations may lead to discrimination of people according to their race, ethnicity or socio-economic status, thus exacerbating exclusion and widening the digital divide. The heavy presence of such data may also make the common origins of stigmatisation (cultural, ethnic, socio-economic) more obvious and even generate new forms of discrimination.

Example from Scenario 3:
Most witnesses said they've suffered from the stress involved in trying to recover their identities and sorting out the mess they've been put in. Some said they've been stigmatised. We heard also about DMC [the Data Mining Corporation] *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.*

Victimisation

Victimisation as a threat is introduced and analysed more in detail in the trust part of the report. However, with regard to the digital divide, the issue of victimisation or the democratic right not to be treated as a criminal as long as one's guilt is not proven can be of consequence, considering the categorisation and thus discrimination and exclusion of users.

Example from Scenario 3:
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.

Credit-reporting agencies raised red flags, not only about the cards, but also 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. …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 …admitted they could never eliminate unreliability nor could their predictions of who might be a terrorist or criminal be 100 per cent.

Voluntary exclusion

Voluntary exclusion is another form of exclusion. It is likely that AmI, like any emerging technology, will be adopted gradually and that some people may consistently refuse to adopt it, thus intentionally excluding or dividing themselves from others. This rejection, a refusal to adopt new technologies, is basically caused by users' lack of trust in or sufficient awareness of new technologies and their implications; it is also sometimes referred to as resistance to change, a sort of inertia displayed by a segment of society to the introduction of radical changes, which may in turn lead to social disruption.

Example from Scenario 4:
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.

4 SAFEGUARDS

This chapter presents a range of safeguards to address the threats and vulnerabilities associated with the key issues of privacy, identity, security, trust and digital divide. Some of these safeguards already exist (e.g., standards, trust marks, etc.), but need to be strengthened in order deal with the threats and vulnerabilities identified in Chapter 3.

4.1 A MATRIX OF SAFEGUARDS

The multiplicity of threats and vulnerabilities associated with AmI will require a multiplicity of safeguards to respond to the risks and problems posed by the emerging technological systems and their applications.[164] In most instances, there is no one-on-one relationship between a certain threat and its specific safeguard. Just as the notion of privacy has different dimensions, so different safeguards will be needed to protect it. Also, just as our notion of trust is context dependent, so those safeguards may also need to be context dependent – which is to say that some safeguards may be acceptable to some people in some countries, but may not be acceptable in other cultural settings. Some safeguards will be applicable in certain situations, but not in others. Moreover, in order to adequately address an identified threat or vulnerability, a combination of several safeguards might be needed; in other instances, a single safeguard has the potential to address numerous treats and vulnerabilities.

The safeguards proposed in this chapter have been grouped into three main approaches, which are, however, not to be understood as a strict separation:

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

The general idea is illustrated in the ensuing table which links a selection of the more than 40 threats and vulnerabilities (vertical axis) which have been discussed in the previous chapter with a variety of corresponding safeguards (horizontal axis) that have been identified to address these and other threats and vulnerabilities. Function creep, for instance, which has been discussed as a major threat to privacy, should not only be addressed by a set of technological safeguards (in this example, the principle of minimal data collection). Arguably, open standards as one of the socio-economic safeguards as well as the principle of purpose limitation from the legal and regulatory sphere can effectively contribute to the impediment of function creep. The problematic lack of awareness of individual users about existing privacy rights is an example of a vulnerability in privacy which can neither be resolved by technical nor legal fixes, but which rather calls for

[164] Other European projects that have dealt or are dealing with some of the same issues as SWAMI have proposed various safeguards. We have referenced these projects in the first SWAMI deliverable, but among those most relevant are ACIP, Ambient Agoras, AMSD, ARTEMIS, BASIS, BIOVISION, eEPOCH, EUCLID, FIDIS, GUIDE, OZONE, PAMPAS, PAW, PISA, PRIME, PROFIT, PROGRESS, RAPID, WWRF. E-Inclusion projects: COST219; Ambient Assisted Living - Preparation of an Art. 169-initiative (AAL) http://www.vdivde-it.de/aal; Conferences, Workshops, Seminars and Tutorials to Support e-Inclusion (CWST) http://cwst.icchp.org/; European Accessible Information Network (EUAIN) http://www.euain.org/; European Internet Accessibility Observatory (EIAO) http://www.eiao.net/; Ambient Intelligence System of Agents for Knowledge-based and Integrated Services for Mobility Impaired users (ASK-IT) http://www.ask-it.org/; Strengthening eInclusion and eAccessibility across Europe (EINCLUSION@EU) http://www.einclusion-eu.org/

actions in the area of education and training. With regard to other threats, such as the issue of high update and maintenance costs which may contribute to the digital divide in AmI, only very few or very weak safeguards – if any – have been identified. The discovery of these lacunae is, of course, an important exercise of its own right as it calls constant attention to research and development in areas that warrant additional activities.

Safeguard / Threat/ Vulnerability		Technological		Socio-economic/ cultural		Legal	
		Minimal data collection	Authorisation and anti-virus software	Open standards	Education/ training	Proportionality and purpose limitation	Effective liability rules
Privacy	Function creep	✓	✓	✓		✓	
	Lack of awareness about privacy rights				✓		
Identity	Identity theft	✓	✓	✓			
	Exploitation of data linkages	✓				✓	✓
Security	Incompatibility of components after system upgrade			✓			
	Malware		✓	✓			
Trust	Lack of transparency			✓			✓
	Denial of service/ discrimination					✓	✓
Digital Divide	High update/ maintenance costs	✓		✓			
	Voluntary exclusion				✓	✓	✓

4.2 TECHNOLOGICAL SAFEGUARDS

Currently, the bulk of research on privacy protection is concerned with user privacy in network applications (such as e-mails and web services, e.g., m-commerce) and also with security of personal devices, and considers privacy protection for current technology settings. The main privacy protecting principles in network applications are

- anonymity (possibility to use a resource or service without disclosure of user identity),
- pseudonymity (possibility to use a resource or service without disclosure of user identity, but still be accountable for that use),

- unlinkability (possibility to use multiple resources or services without others being able to discover that these resources were used by the same user),
- unobservability (possibility to use a resource or service without others being able to observe that the resource is being used).

These principles are fairly clear when users and their data can be spatially separated from each other, as in network applications. However, future AmI settings, described in numerous AmI scenarios (see the first SWAMI deliverable), present more privacy threats than current technology settings.

The main difference between existing network applications and emerging AmI applications is two-fold: first, in the former case, the user has some understanding of which data about him are collected, and has some means to restrict data collection: e.g., to use a public computer anonymously to access certain web pages; to switch off his mobile phone, to pay cash instead of using web service, etc. In the latter case, with the environment full of numerous invisible sensors (which might include video cameras), it is difficult (if not impossible) for users to understand and to control data collection and to achieve unobservability, anonymity and pseudonymity. Indeed, how can pseudonymity be achieved when a full-face image is taken by video cameras used in memory aid applications? Intelligent data processing, limiting linkability and implementing strong access control to collected data, seems to be the main ways of protecting privacy in such applications. However, such applications present potential privacy threats anyway if the police, intelligence agencies or family members can search through memory aid data, and if the owner of the memory aid discovers some interesting facts which he has not paid attention to while changing places or talking to people.

A second important difference between network applications and emerging AmI applications is that neither mobile devices nor web usage penetrates through such strong privacy protecting borders as walls (it is rarely 100 per cent certain who sends a request from a particular IP address or uses a mobile device) and the human body, while physiological, video and audio sensors, proposed for AmI applications, will have much stronger capabilities to identify a person and to reveal personal activities and feelings.

Consequently, future AmI applications in smart environments will require stronger safeguards, many of which are not yet fully developed. We propose research directions for developing privacy-protecting safeguards in future AmI settings.

4.2.1 State of the art

Research on privacy protection

The term “privacy enhancement” has been used for more than a decade to represent technologies concerned with various aspects of Internet security.[165] Privacy protection in Internet applications should be based on the main principles of privacy protection, listed in the Common Criteria for Information Technology Security Evaluation[166] (anonymity,

[165] HiSPEC, *Privacy Enhancing Technologies: State of the Art Review*, Version 1, HiSPEC Report, 2002. http://www.hispec.org.uk/public_documents/7_1PETreview3.pdf.

[166] The Common Criteria (CC) is an international standard (ISO/IEC 15408) for computer security. It does not provide a list of security requirements per se. Instead, it describes a framework in which users can specify their security requirements, developers can make claims about the security attributes of their products, and

pseudonymity, unlinkability and unobservability). The "Handbook of Privacy and Privacy-Enhancing Technologies: the Case of Intelligent Software Agents", published by the **PISA project**, describes how these principles were implemented in a system for agent-based network privacy. An intelligent agent is software that can travel via networks and to do something in a remote host on behalf of a user, e.g., make a search on the Web, book a hotel or buy tickets according to user preferences. Intelligent agents are convenient, but they create a lot of threats to user privacy, which range from revealing user preferences to altering an agent in a malicious way. PISA has pointed out many threats and provided some solutions to them, but not complete solutions. As the authors state in the handbook conclusions, their work has a major limitation: they "assumed that parts of environment are trustworthy and realistically this is most often not the case". In other words, conventional cryptographic techniques are based on the assumption that confidential data can be left unprotected during execution (e.g., during encryption and decryption) because the execution environment is trusted. Consequently, most of conventional cryptography cannot be applied for protection of mobile software, which is executed at untrustworthy hosts.

The **PAW project** is continuing privacy protection research with regard to the use of software agents and works on cryptographic techniques and licensing languages (a description of what one is allowed to do with data during processing and what not). Licensing languages and machine-readable privacy policies are an active research area now, where most research is concerned with privacy policies of Web sites. A recently developed platform for privacy preferences (P3P)[167] allows websites to convey their policies in machine-readable form, so that the policies are checked on the user side and compared with user preferences. However, P3P does not actually force websites to stick to their promises.

The goal of the **PRIME project** is to develop the framework for privacy and identity management in electronic information networks for current settings. Their application areas include eLearning, location-based services and airport security controls. PRIME has developed some very realistic scenarios in future AmI settings (e.g., how an airport environment will look like in AmI future) and point out certain privacy threats, but future settings are not really a project focus. The project has made significant research efforts in the areas of access control (the term "access control" in PRIME stands mainly for access / release / processing of data by software methods, unlike more traditional understanding of the term "access control" as granting rights to a human), cryptography, communication infrastructure as well as user-side and service-side identity management. Access control research is concerned with developing policies for access control and a language for their description, in order to allow users to control use of their personal information and in order to allow negotiations between different counterparts without revealing sensitive information.

Cryptography research is concerned with anonymous credential systems (which allow the user to prove the right to do something anonymously) and use of trusted hardware modules (tamper-resistant hardware tokens to which a credential is bound, so that using the stolen credential from another hardware is prohibited) and other encryption. Communication

---

evaluators can determine if products actually meet their claims. See also Blarkom, G. W. van, J. J. Borking and J. G. E. Olk (eds.), *Handbook of Privacy and Privacy-Enhancing Technologies*: The Case of Intelligent Software Agents, TNO-FEL, The Hague, 2003.

[167] Cranor, L. F., "P3P: Making Privacy Policies More Useful", *IEEE Security and Privacy*, vol. 1, no. 6, 2003, pp. 50-55.

protocols and infrastructure research is concerned with analysis of existing methods to provide user anonymity in Internet, location-based services and sensor networks, and developing of new methods. The conclusion is that "even the most recent techniques and tools are still far from providing a holistic approach to usable and secure anonymising networks".[168]

User-side identity management research has developed a terminology and interfaces for privacy policies (allowing users to specify how their personal data can be used), and proposed that automatic linkability computation (estimation whether an attacker can link to each other two transactions made by the same user or not) can help to increase user privacy. Service-side identity management research is concerned with management of obligations (which force a specified privacy policy to be followed), privacy audit (checking that personal data were processed according to the attached privacy policies) and anonymisation of personal data and information retrieval. The conclusion is that privacy audit and management of privacy obligations present a lot of research challenges and open questions.

The goal of the **FIDIS project** is also to develop privacy-preserving methods of identity management. The FIDIS D 3.3 report, a "Study on Mobile Identity Management", draws usage scenarios (mobile Internet and mobile dating applications) in current technology settings. The project has presented a privacy diamond model for these settings, where the main components are user, device, location and action and the links between them. Thus, four minimal possibilities for an anonymity mechanism are based on hiding links between two components of the model. For example, one option is to hide links between action and device and between action and location by some communication protocol; another option is to hide links between the user and device and the user and location (anonymous use of an Internet café); a third option is to hide links between the user and a device and between an action and location (broadcasts to and from a device, assuming that the users change devices); a fourth option is to hide links between the action and the device and between the user and the location with certain communication protocols such as location-addressing.[169]

Another FIDIS deliverable, D3.1, has presented classification of identity management systems as, first, systems for account management (pure IMS, where the main goal is authentication, authorisation and accounting); second, systems for personalised services which need both user identity and profiles or log histories; third, systems for pseudonym management in, e.g., web services. The deliverable also suggested some good practices for these systems, e.g., for the first type of identity management systems a good practice can be separate access to the user authentication data, user account data and personal data

---

[168] Camenisch, J. (ed.), *First Annual Research Report*, PRIME Deliverable D16.1, 2005. http://www.prime-project.eu.org/public/prime_products/deliverables/rsch/pub_del_D16.1.a_ec_wp16.1_V1_final.pdf. See also Bergstein, Brian, "Research Explores Data Mining, Privacy", The Associated Press, in *The Washington Post*, 17 June 2006. www.washingtonpost.com/wp-dyn/content/article/2006/06/17/AR2006061700387_3.html
Mr Bergstein says, "Intriguing progress appears to have been made at designing information-retrieval systems with record anonymization, user audit logs – which can confirm that no one looked at records beyond the approved scope of an investigation – and other privacy mechanisms 'baked in'." He quotes one researcher as saying that it is technologically possible to bolster security and privacy – "You can kind of have your cake and eat it too." However, he then goes on to say the problem is getting users to change the way in which they deal with information, i.e., to use privacy-enhancing technologies.

[169] Müller, G., and S. Wohlgemuth, *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, 2005. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.3.study_on_mobile_identity_management.pdf.

(address, etc). The deliverable has also suggested architecture of a mobile device security tool for creation of partial identities and using them in wireless and wired networks.[170]

To summarise, the above-listed projects (as well as other privacy/identity projects such as GUIDE and PAMPAS) are mainly dealing with privacy protection in network applications and, to some extent, with protecting personal data stored in personal devices from everybody except for the device owner. However, these projects are not concerned with emerging applications and future AmI settings. For example, if a mobile device serves as a memory aid (a fairly popular application proposal) and has audio/video recording capabilities, it is insufficient to protect data accumulated in a personal device from everybody except the device owner. Additionally, there is a need to protect nearby people from a recording of their personal data by this memory aid.

A survey of some of privacy-enhancing technologies can be found in the HiSPEC report, where it is stated that "more effort in the previous years was invested in protecting user identities rather than personal data".[171] Similarly, the PISA project concludes that the previous research efforts were mainly concerned with the protection of users' identities, but not much of users' actions. These conclusions were made in 2002 (HiSPEC) and 2003 (Blarkom et al.). Since then, research efforts on protection of personal data and user actions have increased. Nevertheless, the PRIME study on the state of the art in privacy protection in network applications, made in 2005, has pointed out many performance problems and security weaknesses.[172]

Privacy protection research is still new, and most efforts are concentrated on data protection for wired and wireless Internet applications. Even in these domains, full privacy-protecting solutions applicable in real life do not exist yet. There is also ongoing research on protection of data stored in personal devices (mainly by means of encryption), but the limited resources of mobile devices present a challenge. For example, automatic encryption of personal data immediately after saving them is difficult because it slows down primary usage of the mobile device. Research on privacy protection in such emerging domains as smart environments and smart cars is in its infancy[173], and only generic guidelines have been developed.

The works of Langheinrich et al. suggest how the fair information practices (listed in current data protection laws) can be applied to AmI applications, and show how difficult it might be to apply them. For example, it is stated that the user must have access to the data stored about him, and the right to change wrong data. In an AmI future, however, it won't be easy for users to find (let alone to check) all pieces of data stored about them in the

[170] Bauer, M., M. Meints and M. Hansen, *Structured Overview on Prototypes and Concepts of Identity Management Systems*, FIDIS Deliverable D3.1, 2005.
http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf
[171] HiSPEC, Privacy Enhancing Technologies: State of the Art Review, Version 1, HiSPEC Report, 2002.
http://www.hispec.org.uk/public_documents/7_1PETreview3.pdf.
[172] Camenish, 2005.
[173] Such research is, however, going on. An example is the EC-supported CONNECT project, which aims to implement a privacy management platform within pervasive mobile services, coupling research on semantic technologies and intelligent agents with wireless communications (including UMTS, Wi-Fi and Wi-Max) and context-sensitive paradigms and multimodal (voice/graphics) interfaces to provide a strong and secure framework to ensure that privacy is a feasible and desirable component of future ambient intelligence applications. The two-year project started in June 2006.
http://cordis.europa.eu/search/index.cfm?fuseaction=proj.simpledocument&PJ_RCN=8292795

network and in the personal devices of surrounding people. Moreover, some data processing techniques (such as neural networks) store user models in a form that is difficult for most people to interpret.[174]

The work of Hong et al. proposes high-level privacy risk models based on two aspects: first, the social and organisational context in which an application is embedded (Who are the data sharers and observers? What kinds of personal information are shared? What is the value proposition for information sharing, symmetry of information sharing, etc.?). The second aspect is technological (How are collection, storage and retention of personal data organised? Who controls the system? Is there any possibility to opt-out?). However, the work mainly suggests guidelines for risk estimation, not for safeguards.[175]

The work of Lahlou et al. focuses "on the specific issues of the data collection phase" and proposes high-level guidelines. One of the most important guidelines is to minimise data collection. Such generic design guidelines as "think before doing" and "understand the way in which new technologies change the effects of classic issues" (i.e., existing solutions in the physical world) can be applied not only to the data collection. However, these generic design guidelines need to be made more specific.[176]

Most of the research on privacy protection is concerned with dangers of information disclosure. Other privacy aspects have not received much attention from researchers. For example, the privacy aspect known as "the right to be let alone" is rarely discussed by technology researchers, despite its importance.

Research on digital divide prevention

Projects dealing with accessibility for all and e-Inclusion (such as COST219: "Accessibility for all to services and terminals for next generation mobile networks", ASK-IT: "Ambient intelligence system of agents for knowledge-based and integrated services for mobility impaired users") are concerned with standardisation, intuitive user interfaces, personalisation, interfaces to all everyday tools (e.g., domotics[177], home health care, computer accessibility for people with disabilities and elderly people), adaptation of contents to the channel capacity and the user terminal and so on.

Standardisation in the field of information technology (including, for example, biometrics) is an important issue in order to achieve interoperability between different products. However, interoperability even in fairly old technologies (such as fingerprint-based

---

[174] Langheinrich, M., "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems", in *Proceedings of the Third International Conference on Ubiquitous Computing* (Ubicomp 2001), edited by G. D. Abowd, B. Brumitt and S. A. Shafer, Springer-Verlag, Berlin, 2001, pp. 273-91; Langheinrich, M., "The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects", Paper presented at the Designing for Privacy Workshop, DC Tales Conference, Santorini, Greece, 2003.

[175] Hong, J. I., J. D. Ng, S. Lederer and J. A. Landay, "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems", in *Proceedings of Designing Interactive Systems (Dis2004),* Boston, MA, 2004, pp. 233-42

[176] Lahlou, S., and F. Jegou, *European Disappearing Computer Privacy Design Guideslines* V1, Ambient Agora Deliverable D15.4, Electricité de France, Clamart, 2003. http://www.ambient-agoras.org/downloads/D15[1].4_-_Privacy_Design_Guidelines.pdf

[177] Domotics is the application of computer and robot technologies to domestic appliances. Information and communication technologies are expected to provide for more comfort and convenience in and around the home. www.domotics.com/

identification) has not yet been achieved. The ISO is developing standards for storage of biometric data, including fingerprint data. However, the ILO Seafarer's Identity Documents Biometric Testing Campaign Report has demonstrated that commercial fingerprint devices have poor interoperability, despite the standards.[178]

Another important problem is translation from one language to another, mainly from English to other languages (currently, it is not easy to find information on the Web without a good knowledge of the English language). Language translation software is not yet able to cope with complex language constructions.

4.2.2 Minimal data collection, transmission and storage

Minimising personal data should be factored into all stages of collection, transmission and storage systems. The goal of the minimal data transmission principle is that data should reveal little about the user even in the event of successful eavesdropping and decryption of transmitted data. Similarly, the principle of minimal data storage requires that thieves don't benefit from stolen databases and decryption of their data. Implementation of anonymity, pseudonymity and unobservability methods helps to minimise system knowledge about users at the stages of data transmission and storage in remote databases, but not in cases involving data collection by and storage in personal devices (which collect and store mainly data of the device owner) or storage of videos.

The main goals of privacy protection during data collection are, first, to prevent linkability between diverse types of data collected about the same user and, second, to prevent surveillance by means of spyware or plugging in additional pieces of hardware transmitting raw data (as occurs in wiretapping). These goals can be achieved by

- careful selection of hardware (so that data are collected and transmitted only in the minimally required quality and quantity to satisfy an application's goals, and there are no easy ways to spy on raw and processed data);
- an increase of software capabilities and intelligence (so that data can be processed in real time); and
- deleting data as soon as the application allows.

In practice, it is difficult to determine what "minimally needed application data" means. Moreover, that data can be acquired by different means. For example, systems for recommending movies need to know the user's opinion about videos in order to improve the quality of recommendations, and users' laziness in providing feedback is a well-known problem for such systems. Implicit (without asking users to rate a video) user feedback can be acquired by different methods, for example, by processing audio signals while a user watches a video in an attempt to understand the user's reaction and to assess the user's opinion from the collected audio data; analysing a user's behaviour (e.g., fast forwarding a video) while the video is played; analysing a user's facial expressions and physiological signals. User feedback data are needed for movie recommendation systems, but collection of such data can present different privacy threats depending on which sensors are used – physiological and video sensors are the most privacy-threatening.

[178] International Labour Organization, *ILO Seafarers' Identity Documents Biometric Testing Campaign Report*, Part 1, ILO, Geneva, 2004.
http://www.ilo.org/public/english/dialogue/sector/papers/maritime/sid-test-report1.pdf

Software capabilities need to be maximised in order to minimise storage of raw data and avoid storage of data with absolute time stamps. We suggest this safeguard in order to prevent accidental logging of sensitive data, because correlation of different kinds of data by time stamps is fairly straightforward.

These safeguards are presented below in more detail:

- In our opinion, the most privacy threatening are physiological sensors and video cameras. Physiological sensors are privacy threatening because they penetrate deeply inside the human body and can reveal health data and personal feelings. Video cameras, especially those storing raw video data are privacy-threatening because they violate people's expectations that "nobody can see me if I am hidden behind the wall" and because playback of video data can reveal more details than most people pay attention to in normal life. We suggest that usage of these two groups of devices should be restricted to safety applications until proper artificial intelligence safeguards (see below) are implemented.
- Instead of logging raw data, only data features (data features are a limited set of pre-selected characteristics of data, e.g., frequency and amplitude of oscillations) should be logged. This can be achieved by using either hardware filters or real-time pre-processing of data or a combination of both. For example, health care applications should log only the number of peaks where the user's heart rate is above a predefined threshold, or the time period when the heart rate was high; gaming application should detect predefined contexts and user actions in real time, e.g., certain set of commands) and so on.
- Time stamping of logged data should be limited by making it relative to other application-related information (e.g., "In the first hour after taking a pill, the blood pressure was normal, then it started to increase.") or by averaging and generalising time-stamping (e.g., "Blood pressure was above threshold for two hours a day."). Time stamping in this way would prevent the discovery of personal information, e.g., a young man's heart rate is elevated each time he meets a certain young woman.
- Hardware used for data collection should not have extra memory and extra data transmission capabilities, and no easy plug-ins for increasing them. Such a minimalist hardware approach can help against spying and could be achieved by, for example, giving to each application access rights to a certain memory block instead of giving to all applications access to the same main memory.
- Data should be deleted after an application-dependent time, e.g., when a user buys clothes, all information about the textile, price, designer, etc., should be deleted from the clothes' RFID tag. For applications that require active RFID tags (such as for finding lost objects[179]), the RFID identifier tag should be changed, so that no links between shop database and personal clothes are left.
- Applications that don't require constant monitoring should switch off automatically after a certain period of user inactivity (for example, video cameras should automatically switch off at the end of a game).
- Anonymous identities, partial identities and pseudonyms should be used wherever possible. Using different identities with the absolute minimum of personal data for each application helps to prevent discovery of links between user identity and personal data and between different actions by the same user. For example, if a user buys something and has paid for it in advance, it should be possible for the user to stay anonymous. If the

[179] Orr, R. J., R. Raymond, J. Berman and F. Seay, "A System for Finding Frequently Lost Objects in the Home", *Technical Report 99*-24, Graphics, Visualization, and Usability Center, Georgia Tech, 1999.

user cannot stay completely anonymous, he should be provided with different pseudonyms for different applications. This is needed in order e.g. to prevent a discovery (either by personal contact details, or by ID of a personal device) that a person who has ordered a box of chocolates is the same who has ordered diabetes-related medicines. Such a discovery would allow an insurance company (for example) to conclude that the diabetic client is not following a prescribed dietary regime and therefore his insurance premiums should be increased. However, currently the ID of a personal device can be discovered easily in many cases. Partial identities can be used only in applications in which personal data can be physically separated from personal identity, typically in network applications and databases. Partial identities and anonymity are not achievable if, e.g., raw video data are stored or if user preferences are stored in the personal device.

4.2.3 Data and software security

For the purpose of this section, by security, we imply means of data and software protection from malicious actions (e.g., data theft, modifications of program code, etc.), and not security in wider sense, which in fact can endanger privacy. For example, surveillance of all people in the country might increase security by making it more difficult for criminals to act, but such surveillance would also violate our privacy.

Data and software protection from malicious actions should be implemented by intrusion prevention and by recovery from its consequences if they happen. Intrusion prevention can be active (such as antivirus software, which removes viruses) or passive (such as encryption, which makes it more difficult to understand the contents of stolen data).
At all stages of data collection, storage and transmission, malicious actions should be hindered by countermeasures such as the following:

- *cryptography*: reliable encryption of program code, identity data and all personal data, which should work on any untrustworthy platform. Code encryption should allow the code to be executed in its encrypted form[180]; currently code encryption does not work for arbitrary functions and situations;
- *watermarking*: a method to conceal a message in such a way that the very existence of the embedded message is undetectable, e.g., the copyright is embedded into multimedia objects for protecting them against illegal copying. Watermarking can also be used for software protection. In this case, a special data structure is embedded in the program so that even after the execution of the program, this special data structure still exists and makes it possible to detect any malicious modification of the program;
- *anti-virus software and firewalls*;
- *automatic updates of antivirus and firewall software*. Since a personal device usually contains data about many people (contact details, photos, parts of schedules of friends, colleagues and family members), and since one malicious node can endanger many other nodes in a network, proper protection of data and software contained in each personal device is actually a societal problem and not just a problem for the device owner. Consequently, we suggest that updates of anti-virus software be automatic, i.e., the user should not need to take any actions to get the updates (his or her service provider or software supplier should, however, notify the user when there is an update). Updates of virus signatures should be provided free of charge. Otherwise, there will be many people who forget or don't have time or money to update their device software in time, and this can endanger the data of their family, friends or colleagues. For example,

[180] Blarkom et al., 2003, p.81.

service providers can take care of the anti-virus software of their clients (see section on socio-economic safeguards). However, it is important to take care that these software updates are compatible with existing system configurations, otherwise they can be dangerous (cf. section on security threats);

- *self-healing methods for personal devices.* Currently, only life-critical applications are highly reliable and have redundant blocks and built-in watchdogs that restart the application if something goes wrong. It would be useful if personal devices had redundancy built into their most important functionalities and if they employed internal watchdogs in order to switch to these redundant functionalities in the event of suspicious execution delays or spyware detection;
- *detection of changes in hardware configuration*, i.e., when hardware is removed, replaced or upgraded and/or when plug-ins are added. Cases involving small devices without a user interface (such as wireless network nodes) should be reported to the administrator (because replacing a node's hardware might imply that the node's data are no longer trustworthy). In cases involving devices with a user interface, authorisation by and/ or reporting to the administrator should be required.
- *usage of trusted hardware modules*: a piece of hardware dedicated to the protection of secret data and firmly attached to a personal device (e.g., soldered to the motherboard of a notebook PC). For example, such a piece of hardware may contain an encryption key, so that private data can only be decrypted with a trusted hardware module, and not far away from it.
- *secure establishing of ad hoc communications* and possibility of encrypted ad-hoc communications (e.g., if somebody needs to print a sensitive document with a public printer, the document should be sent to the printer in encrypted form to avoid eavesdropping, which is difficult to achieve).

4.2.4 Privacy protection in networking (transfer of identity and personal data)

Data transfer in AmI applications takes place between remote locations (e.g., in m-commerce applications or web browsing), as well as between diverse sensors in a smart space and between devices which belong to a Personal Area Network (PAN), e.g., several sensors attached to a human body or embedded in personal belongings. In all transfers, the data should be secure (see previous section) and protected from malicious actions such as eavesdropping, data modifications and denial of service by security measures (see previous section and by access control methods (see the next section).

Additionally, privacy protection in networking includes providing anonymity, pseudonymity and unobservability whenever possible. When data is transferred over long distances, anonymity, pseudonymity and unobservability can be provided by the following methods: first, methods to prove user authorisation locally and to transmit over the network only a confirmation of authorisation; second, methods of hiding relations between user identity and actions by, e.g., distributing this knowledge over many network nodes. For providing anonymity, it is also necessary to use special communication protocols which do not use device IDs or which hide them. It is also necessary to implement authorisation for accessing the device ID: currently most RFID tags and Bluetooth devices provide their IDs upon any request, no matter who actually asked for the ID. Another problem to solve is that devices can be distinguished by their analogue radio signals, and this can hinder achieving anonymity. Additionally, by analysing radio signals and communication protocols of a personal object, one can estimate the capabilities of embedded hardware and

guess whether this is a new and expensive thing or old and inexpensive, which is an undesirable feature.

Unobservability can be, to some extent, implemented also in smart spaces and PANs by limiting the communication range so that signals do not penetrate through the walls of a smart space, or of a car, unlike the current situation when two owners of Bluetooth-enabled phones are aware of each other's presence in neighbouring apartments.

Methods of privacy protection in network applications (mainly long-distance applications) include the following:

- *anonymous credentials* (methods to hide user identity while proving the user's authorisation), e.g., blind signature: a form of digital signature, but with one critical feature added, the capability to hide user identity. The only thing the recipient is aware of is that the transmission has been authenticated. Blind signatures are used for "digital cash" applications, which allow anonymous payments. Blind signatures are also used for building digital pseudonyms. As with other digital signatures, blind signatures are based on encryption techniques, such as public key encryption techniques.
- *a trusted third party*: an independent entity trusted by both the user and service provider which preserves the relationships between the user's true identity and his/her pseudonym, and is permitted to reveal a true user identity only under certain conditions.
- *zero-knowledge techniques*: allow one to prove the knowledge of something without actually providing the secret (e.g., to prove knowledge of a password without actually revealing it).
- *secret sharing schemes*: methods of sharing a message among a set of participants in such a way that any subset of participants can reconstruct the message provided that the subset size is larger than a predefined threshold. Any smaller subset cannot reconstruct the message.
- *special communication protocols and networks*
  - *onion routing*: messages are sent from one node to another so that each node removes one encryption layer, gets the address of the next node and sends the message there. The next node does the same, and so on until some node decrypts the real user address. The effect is that all nodes need to co-operate in order to find out the user's real address. The drawback is that message size changes with each removal of an encryption layer, and this allows certain tracking of messages.
  - *Mix networks and crowds*. The idea is to hide the relationship between senders and receivers by having many intermediate nodes between them. These intermediate nodes collect several incoming messages, mix them and forward to the next node until the last node, which sends the message to the real address. Nodes can also generate random traffic in order to hide real messages. However, these protocols suffer from latency problems (a sufficiently large number of messages need to accumulate in one node before they are forwarded); they require a large number of active senders and receivers and large buffers of mixing nodes.
- *communication protocols which do not use permanent IDs* of a personal device or object; instead, IDs are assigned only for the current communication session (otherwise it is easy to associate a device or an object, e.g., eye glasses, with a user because such things as phones, eye glasses or credit cards are really personal). Communication protocols that provide anonymity at the network layer, as stated in the PRIME

deliverable[181], are not suitable for large-scale applications: there is no evaluation on desired security level, and performance is a hard problem.

A policy battle is brewing between governments such as the UK which want access to encryption keys and encryption advocates such as Phil Zimmerman. The latter has recently posted on his website free software for encrypting computer-to-computer telephone calls.[182] Called Zfone, his software performs the key exchange inside the digital voice channel while the call is being set up, so no third party has the keys. Meanwhile, the UK government is preparing to give the police the legal authority to compel both organisations and individuals to disclose encryption keys.

4.2.5 Authorisation and access control

The traditional understanding of the term "access control" is with respect to people, i.e., granting a person the right to log in or enter an office. Proper methods of access control are also needed in AmI applications. Physical access control is required in applications such as border control, airport check-ins and office access. Access control methods are required for logging on to computers and personal devices as well as network applications such as mobile commerce, mobile voting and so on. There is a growing need to employ reliable authentication methods instead of passwords as commonly used today. However, often it is assumed that an authentication method is reliable if its error rate is low, as it is, for example, in the case of iris and fingerprint recognition. This belief leads to a problem that if an impostor succeeds in being verified by such a method once, he can do whatever he wants.

Thus, reliable authentication should have low error rates *and* strong anti-spoofing protection. Work on anti-spoofing protection of iris and fingerprint recognition is going on, but spoofing is still possible.

We suggest that really reliable authentication should be unobtrusive, continuous (that is, several times during an application-dependent time period) and multimodal. It is more difficult to spoof several biometric modalities than only one. If a car lock can only be opened by the car owner's fingerprint, criminals may either produce a faked fingerprint sample or cut off the owner's finger. However, if authentication of the owner continues inside the car (e.g., by weight sensors embedded in the seat, by the relative position of the seat and mirrors, by driving patterns, by voice or even by face recognition), the impostor will be discovered sooner or later. Consequently, stealing cars will not be so attractive.

So far, there has been limited research on continuous multimodal access control systems. Also most access control methods don't help against a dishonest authorised person stealing data. Artificial intelligence safeguards (see below), however, may help.

Recently, the meaning of the term "access control" has broadened to include checking which software is accessing personal data and how the personal data are processed. This should be achieved by developing ways to express legal requirements and personal user wishes in machine-readable rules and by embedding these rules into personal data in such a

[181] Camenish, 2005
[182] Markoff, John, "Voice Encryption May Draw U.S. Scrutiny", *The New York Times*, 22 May 2006. http://www.nytimes.com/2006/05/22/technology/22privacy.html?_r=1&oref=slogin

way that they cannot be ignored or bypassed (much the same way as digital rights management methods are designed to prevent illegal copying of files).

Authentication methods include the following:

Biometrics

Biometrics in identity management means using measurable physiological and behavioural characteristics to identify persons (i.e., to recognise one person out of many possible options) or to verify (authenticate) a user (i.e., to confirm that the user is the person whom he claims to be). Currently, the most reliable physiological biometrics are iris and fingerprint recognition, while face, voice and hand geometry recognition are less reliable. It is also possible to verify a person by so-called "soft" biometrics (e.g., height and weight), which are not very reliable methods. Behavioural biometrics-based verification can use personal walking style (gait), signature, patterns of computer mouse or keyboard usage and so on.

Biometrics offer several advantages:

- Convenience: biometrics are always with a person, so there is no need to remember passwords or to carry smart cards.
- Biometrics allows unobtrusive (unnoticeable) person identification, e.g., to identify a burglar by video taken by security cameras.
- Biometrics are assumed to be a more reliable means of user verification than passwords or smart cards, because it is more difficult to fake a fingerprint than to steal a smart card.

However, biometrics also have certain disadvantages:

- Spoofing of biometric sensors is not impossible. The work of Daugman shows that many modern iris recognition sensors can be spoofed simply by a picture of an iris printed on paper. Ways of faking fingerprint are widely known and even published on the Web.[183]
- Biometrics carry a high risk of identity theft, i.e., the risk that personal biometric data will become known to a criminal, the corresponding biometric sample will be faked and used for gaining access to a computer or a building or for compromising the person; and recovering from theft of a fingerprint or iris image is more difficult than from smart card loss because people have only 10 fingers and two eyes.
- Moreover, the use of biometrics also increases the risks to the health and life of the victim of a crime, because the attacker changes his tactics, which may be more harmful, for example, if a criminal cuts off a person's finger in order to open the biometric lock on his car.[184]

These disadvantages could be overcome. For example, anti-spoofing measures could include the following solutions:

- multi-modal biometrics (using two or more biometric modalities for verification or identification). It is more difficult to spoof several biometric sensors than only one; in

[183] Daugman, J., "Iris Recognition: Anti-spoofing Liveness Testing, Stable Biometric Keys, and Further Research Directions", in *BioSecure 1st Residential Workshop*, Paris, August 2005.

[184] Schneier, B., *Beyond fear: Thinking sensibly about security in an uncertain world*. Copernicus Books, New York, 2003. Lettice, J., "Carjackers swipe biometric Merc, plus owner's finger", *The Register*, 4 April 2005. http://www.theregister.co.uk/2005/04/04/fingerprint_merc_chop/

addition, recognition rates of multimodal biometric systems are usually higher than if each single modality is used alone.
- liveness detection (which aims to distinguish a living person from fake biometric samples and from biometric samples separated from the human body). This is not a mature technology yet.

There is, however, some concern among experts that biometrics should not be the focus of the security approach in a AmI world, since the identification and authentication of individuals by biometrics will always be approximate, is like publishing passwords, can be spoofed and cannot be revoked after an incident.[185] (Engberg 2006; Pfitzmann 2006)

Tokens

Tokens are portable physical devices given to users who keep them in their possession. They can be read directly like a credit card, or they may display a changing number that is typed in as a password. They can also hold biometric data, so that a biometric sample of the user is compared to the biometric template stored in a token, instead of being compared with the template stored in a central database. The main disadvantage is that it is fairly easy to lose or to steal a token. Tokens made in a form of a card (similar to a credit card) can be broken.

Implants

Implants are small physical devices, embedded into a human body (nowadays they are inserted with a syringe under the skin). Implants are used for identification by unique ID number, and some research aims to add a GPS positioning module in order to detect the user's location at any time.

Multimodal fusion

With multi-modal fusion, identification or authentication is performed by information from several sources, which usually helps to improve recognition rates and anti-spoofing capabilities. These sources can be biometric sensors: either different biometric modalities (a popular combination of modalities is face and voice) or different methods of processing data from the same biometric modality (for example, three-dimensional and two-dimensional face recognition). Multimodal identification and/or authentication can also be performed by combining data from biometric modalities and non-biometric data, e.g., biometrics and a password are required at the same time, or biometrics plus location information, or a biometric is stored in the token along with the token's ID. Tokens and implants have an advantage in that they are easier to replace than biometrics (biometrics, if compromised, can not be used any longer, and the number of biometric identifiers of a human is limited) and a disadvantage in that they, especially tokens, are easier to steal.

In cases when reliable personal authentication is needed, multimodal authentication should be used. Methods for reliable unobtrusive authentication (especially for privacy-safe unobtrusive authentication) should be developed. Current state of the art in authentication

[185] See, for example, Engberg, Stephan, "Empowerment and Context Security as the route to Growth and Security", and Pfitzmann, Andreas, "Anonymity, unobservability, pseudonymity and identity management requirements for an AmI world". Both papers were presented at the SWAMI Final Conference, Brussels, 21-22 March 2006 and can be found at http://swami.jrc.es.

is such that reliable authentication requires explicit user effort, while unobtrusive authentication is not reliable. Moreover, most efforts in unobtrusive authentication are devoted to face and voice recognition, which is privacy-threatening because the facial image and voice need to be captured. As mentioned above, it is also possible (although not so reliable) to verify the user by patterns of mouse and keyboard usage[186], by weight, height, body fat percentage[187], by gait[188] and probably some other not so privacy-threatening features. Multimodal verification by several unobtrusive modalities should increase reliability; however, unobtrusive privacy-safe biometrics and multimodal biometric fusion are fairly young research areas, and not mature yet.

Unobtrusive authentication should enable greater security because it is more user-friendly. People are not willing to use explicit authentication frequently, which reduces the overall security level, while unobtrusive authentication can be used continuously. For example, if a person works with large databases of sensitive data, continuous unobtrusive authentication (e.g., by patterns of mouse usage) would prevent a situation where an impostor succeeds in spoofing the system once (e.g., with a faked fingerprint and stolen implant) and after that gets full access to sensitive information. Continuous unobtrusive user verification (e.g., by voice and gait) is needed for protection of personal devices. Currently personal devices (especially mobile phones) are unprotected for a long time after a user has switched on the device, because users are unwilling to use explicit verification protection frequently (such as typing a password or giving a fingerprint) and because of the inconvenience of having to switch off the phone before it requires user verification.

Access control should be context-dependent, requiring more reliable authentication if a user spends more money than usual (or above a predefined threshold), or if a mobile user is in a foreign location. Such context-dependent authentication is not yet mature for real-life use, especially because current authentication methods are mainly explicit and not really multimodal.

Access control to software (data processing methods) is needed for enforcing legal privacy requirements and personal privacy preferences. Such access control methods are being developed, and include:

- *privacy policies*: methods, which allow users to specify how their personal data can be processed. One recently developed standard is the platform for privacy preferences (P3P), which allows websites to convey their policies in machine-readable form, so that the policies are checked at the user side and compared with the user preferences. However, P3P does not actually force websites to follow their promises. In P3P it is supposed that a personal privacy policy should be created once on a personal device; and after that, the personal device should check that a web site's policy complies with the user-specified policy, negotiate the cases when it does not and warn the user if negotiation fails. We think that it can be burdensome or even hopeless for users to deal

[186] Ahmed, A. A. E., and I. Traore, "Anomaly Intrusion Detection based on Biometrics", *Proceedings of the 2005 IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY, June 2005.

[187] Ailisto, H., E. Vildjiounaite, M. Lindholm et al., "Soft Biometrics – Combining Body Weight and Fat Measurements with Fingerprint Biometrics", *Pattern Recognition Letters*, vol. 27, 2006, pp. 325-334.

[188] Nixon, M., J. Carter, J. Shutler and M. Grant, "New Advances in Automatic Gait Recognition", *Elsevier Information Security Technical Report*, vol 7, No. 4, 2002, pp. 23-35; Ailisto, H., M. Lindholm, J. Mantyjarvi et al., "Identifying people from gait pattern with accelerometers", in E. M. Carapezza (ed.), *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IV*, Proceedings of the SPIE, 5779, 2005, pp. 7-14.

with such warnings. Even in cases of web usage, if the user needs some information, he will most probably sacrifice some private data to the first website capable of providing such information instead of spending time finding another website. Such behaviour will be even more common if the whole environment is full of possibilities whereby user privacy may be violated. If the user has specified that he does not want his image to be recorded, but there are many video cameras in the user's workplace, the warnings will have little effect;

- *user-friendly interfaces* for providing awareness and configuring privacy policies. Maintaining privacy is not at the user's focus, so privacy information should not be a burden for a user. On the other hand, if the user is really concerned about protecting his privacy, he should easily be able to know and configure the following important settings:
  - the purpose of the application goal (e.g., recording a meeting)
  - how much autonomy the application has (what it can do on its own initiative and in which cases, e.g., to start recording when all meeting participants arrive; to suggest that a medicine be taken at a certain time of the day)
  - the information flow from the user, who should be able to understand and to configure the following:
    - what data are collected and how (e.g., continuous record of blood pressure vs. counting number of high blood pressure peaks)
    - what happens to the data after collection (what is processed locally, what is transmitted, what is stored and where, for how long the data are stored)
    - what patterns are searched in the data
  - the information flow to the user, who should be able to configure the following:
    - how the information is presented (e.g., should a reminder to take a medicine be given in audio form or via SMS)
    - how the information is filtered (e.g., an application for personalisation of advertisements could completely block advertisements which it considers uninteresting to the user, or it could present the complete list of advertisements ranked by their estimated usefulness);
- *standard concise methods of initial warnings, similar to the form of road signs*, which indicate whether most privacy-violating technologies (such as those that record video and audio data, log personal identity data, physiological and health data, etc.) are used by ambient applications. For example, signs on the door of a shop can warn customers about video cameras inside the shop, as is now often the case, but there are no signs on mobile phones which inform their owners about their position location capabilities. Unlike standardisation of privacy policies for a web site, which has already started, development of user-friendly transparency tools applicable to all AmI components has not started yet;
- *user-friendly interfaces for fast and easy control over the environment that can override previous settings*, if needed. For example, if a criminal has entered somebody's home and the owner is hiding, an automatic switching on of the lights in a room that senses the presence of people can help the criminal to find and kill the owner. Thus, the owner should be able to disable automatic lighting on very quickly. On the other hand, this action should require some fast authentication in order to prevent the criminal from being able to switch on the lights again;
- *licensing languages*: ways to express legal requirements and user-defined privacy policies in such a way that they can be attached to personal data for the lifetime of their transmission, storage and processing. These methods should describe what can be done with the data in different contexts (e.g., in cases involving the merging of databases),

and to ensure that the data are really treated according to the attached licence. These methods should also facilitate privacy audits (checking that data processing has been carried out correctly and according to prescribed policies), including instances when the data are already deleted. These methods should be tamper-resistant, similar to watermarking. Researchers are just starting to develop licensing tools, but they are not mature yet, e.g., attaching licences to data and checking the merger of databases are dark areas, expressing legal requirements in machine-readable form is difficult, and so on.

4.2.6 Generic architecture-related solutions

The main goal of high-level application design is to provide an appropriate level of safeguards for the estimated level of threats. This can be achieved by proper data protection (e.g., by encryption or by avoiding usage of inexpensive RFID tags which do not have access control to their ID) and by minimising the need for active data protection on the part of the user (e.g., by broadcasting advertisements so that each personal device can select the most interesting ads for its owner, instead of revealing personal preferences by querying shops).

High-level application design should also consider what level of technology control is acceptable (i.e., is the application smart enough to do anything autonomously or to make proactive suggestions) and should provide easy ways to override automatic actions. High-level design should thoroughly test AmI systems, because with diversity of software and hardware providers and with the growing complexity of systems, the possibility of something unpredictable happening increases dramatically. Good design should also consider how the user can escape from using the AmI system in such a way that it is not harmful to him. For example, currently people understand that mobile phones are not always with their owners (e.g., the owner can forget or lose the phone). Thus, if someone calls an acquaintance and the call is not answered, the calling person is not able to find out the reason for not the call being answered. The phone owner can always ignore annoying calls and apologise for them later by saying “Sorry, I was in the shower” or “Sorry, it was so noisy around that I did not hear the phone ringing.” Nowadays, children often “forget” their mobile phones at home or “forget” to switch on the ring tone if they want to escape from parents’ attention. However, in the future, when communication capabilities will move closer to the human body (e.g., embedded in clothes, jewellery or watches), and battery life will be longer, it will be much more difficult to pretend that one has not heard an unwanted call or to avoid being captured by ubiquitous sensors). It is an open question how society will adapt to such increasing transparency, but it would be beneficial if a graceful exit from AmI technologies were possible and if it were possible to escape in a way that was not regarded as anti-social.

Another point to consider with regard to AmI architecture design is the trade-off between device capabilities and price. For example, the small screens of today’s mobile phones present privacy protection problems, because privacy polices or warnings might not fit there. Similarly, advanced antivirus and advanced reasoning algorithms can be costly and can require more memory. However, they are important for privacy protection.

To summarise, the points to consider in system design are these:

- Data filtering on personal devices is preferred to data filtering in an untrustworthy environment. For example, instead of the user having to send his financial preferences

to a jewellery shop, an application could query the shop about all items, and filter them by price and other criteria already on the personal device. Admittedly, this would require more data transmission and does not allow the use of certain efficient recommended techniques known as collaborative filtering, but it has the advantage that users don't feel irritated by the fact that a piece of metal decides what can they afford. Still another way can be the design of services (e.g., location-based services) in such a way that personal devices do not have to send queries; instead, services simply broadcast all available information to devices within a certain range. Such an implementation can require more bandwidth and computing resources, but is safer because it is unknown how many devices are present at a location. Thus, it is more difficult for terrorists to plan an attack in the location where people have gathered.

- Authorisation should be required for accessing not only personal data stored in the device, but also for accessing device ID and other characteristics, which is not currently the case with many technologies. Since devices are associated with one user or one object, knowing the ID of a personal device or the ID of a personal object makes it possible to track the user. For example, many RFID tags, even the most sophisticated of them, including those to be embedded in passports, don't have any access control to their unique IDs, even if they have access control to the data stored in the tag's memory[189]. The same applies to Bluetooth communication: Bluetooth-enabled device sends its ID in response to a request from another Bluetooth-enabled device without considering whether it is authorized to receive the ID. Consequently, thieves can detect whether the owner of a Bluetooth-enabled device is at home or not, especially because signal strength is often sufficient to establish communications through the walls.
- Good design should enable detection of problems with hardware (e.g., checking whether the replacement of certain components was made by an authorised person). Currently mobile devices and smart dust nodes don't check anything if the battery is removed, and do not check whether hardware changes were made by an authorised person, which makes copying data from external memory and replacement of external memory or sensors relatively easy.
- Personal data should be stored not only encrypted, but also split according to application requirements in such a way that different data parts are not accessible at the same time. For example, a "paying salary" application needs to know only bank account number, salary and taxes, but it does not need to know the user name, address, credit card number and so on. Consequently, access to the different applications should be different.[190]
- An increase in the capabilities of personal devices is needed for many reasons. An increase in processing power should allow some redundancy (consequently, higher reliability) in implementation and it should allow powerful multi-tasking: simultaneous encryption of new data and detection of unusual patterns of device behaviour (e.g., delays due to virus activity). An increase in processing power should also allow more real-time processing of data and reduce the need to store data in raw form. An increase in screen size (possibly by enabling folded displays) would ease development of user interfaces. With larger screen size and better resolution, users will be able to read more text at once, which provides a better opportunity to inform users about privacy threats and policies.

[189] Knospe, H., and H. Pohl, "RFID Security", in *Elsevier Information Security Technical Report*, vol. 9, No. 4, 2004, pp. 30-41.

[190] Stajano, F., "One user, many hats; and, sometimes, no hat – towards a secure yet usable PDA", *Proceedings of Security Protocols Workshop 2004*, LNCS, Springer-Verlag, Berlin, 2004.

- Software should be tested by trusted third parties. Currently there are many kinds of platforms for mobile devices, and business requires rapid software development, which prevents thorough testing of security and the privacy-protecting capabilities of personal devices. Moreover, that privacy protection requires extra resources and costs.
- Good design should provide the user with easy ways to override any automatic action, and to return to a stable initial state. For example, if a personalisation application has learned (by coincidence) that the user buys beer every week, and includes beer on every shopping list, it should be easy to return to a previous state in which system did not know that the user likes beer. Another way to solve this problem might be to wait until the system learns that the user does not learn beer. However, this would take longer and be more annoying.
- Good design should avoid implementations with high control levels in applications such as recording audio and images as well as physiological data unless it is strictly necessary for security reasons.
- Means of disconnecting should be provided in such a way that it is not taken as a desire by the user to hide.

4.2.7 Artificial intelligence safeguards

To some extent, all software algorithms are examples of artificial intelligence (AI) methods. Machine learning and data mining are traditionally considered to belong to this area. In context of this SWAMI report, however, we regard AI as potential safeguards with very advanced reasoning capabilities. Although AI safeguards are not yet mature solutions, research is actively going on.

Many privacy threats arise because the reasoning capabilities and intelligence of software have not been growing as fast as hardware capabilities (storage and transmission capabilities). Consequently, the development of AI safeguards should be supported as much as possible, especially because they are expected to help protect people from accidental, unintentional privacy violation, such as disturbing a person when he would not want to be, or from recording some private action. For example, a memory aid application could automatically record some background scene revealing personal secrets or a health monitor could accidentally send data to "data hunters" if there are no advanced anti-spyware algorithms running on the user's device. Advanced AI safeguards could also serve as access control and anti-virus protection by catching unusual patterns of data copying or delays in program execution.

We recommend that AmI applications, especially if they have high control level, should be intelligent enough to:

- detect sensitive data (e.g., recognition that persons in a photo are naked or kissing; or that a conversation is private, even if it takes place in an office) in order to avoid recording or publishing such data;
- adapt to a person's ethics (e.g., not to take photos of naked persons automatically; not to remind about private obligations, e.g., taking medicines, in public; not to record personal conversations, respect human dignity);
- adapt to common sense (e.g., not to disturb a tired person without a serious reason; not to give similar instructions to a three-year-old child and to a teenager)
- adapt to different cultures and etiquettes for understanding privacy-protecting requirements and for the right way to deliver online courses. First, privacy is culture-dependent, e.g., accidentally publishing a photo of a Muslim woman with an uncovered

head or arms is privacy-violating, while publishing a photo of an actress in erotic video is just a part of her advertising. Second, for successful interactions with students, e-learning software should adapt information presentation and interpretation of students' feedback to their cultures in order to avoid misunderstandings and to facilitate acceptance of AmI applications (e.g., current research on user interfaces (UI) suggests that UI colours, page layout, selected pictures and computer voice, let alone jokes, are different for different cultures) and so on;

- summarise intelligently online records, e.g., online conversion of a meeting audio stream into a text document, including only working discussions;
- interpret intelligently user commands with natural interfaces: the application should have means to resolve ambiguities (e.g., to understand when the user addresses the application, and when he/ she talks to other people, and to be able to understand complex language constructions in any context), otherwise, a reply to a someone's question, misinterpreted as a reply to a computer's question, could create a privacy-threatening situation;
- provide language translation tools capable of translating ambiguous expressions; otherwise, providing online information and education for all will be impossible, and digital device between people who know many languages, and non-English speaking people who know only own language is inevitable
- detect unusual patterns of copying and processing of personal data (e.g., if a back-up of data takes place soon after the previous back-up, it may indicate data theft and an alarm should be given). This safeguard should help also when a person authorised to work with the data is dishonest, unlike other access control methods which work mainly against outsiders;
- provide an automatic privacy audit, checking traces of data processing, data- or code-altering, etc.

Research on all of the above-listed topics is going on, and although solutions are not mature for real-life use yet, finding solutions to these problems does not seem less realistic than to realise the vision of the ISTAG scenarios of "Dimitrios" and "Annette and Solomon" which suggested that AmI could replace a secretary (e.g., to discuss problems with Dimitrios' wife on behalf of Dimitrios and without his even being aware of his wife's call) and a teacher.

These requirements are not easy to fulfil in full scale in the near future; however, we suggest that it is important to fulfil these requirements as much as possible. To some extent, these requirements can be fulfilled already nowadays, by setting common sense-based rules (e.g., a rule that situations involving the presence of only one or two persons be considered as potentially a greater privacy risk than situations involving many people) and by reducing the application's control level. One example: in case of an application that could provide summaries of meetings, only words spoken into a microphone should be recorded. This solution has the drawback that users have to switch on microphones before starting to talk. Some comments made without the microphones switched on would be lost, but it is more privacy-safe. An application that takes photos automatically should not take photos, unless otherwise instructed, if just one or two persons are present, and so on.

4.2.8 Recovery means

It seems quite probable that data losses (e.g., in 2002, mobile phones in the UK were stolen every three minutes[191]; and mobile phones contain a lot of personal and business data) and identity thefts, which present serious problems nowadays, will continue into the future. However, losses of personal data will be more noticeable in the future because of the growing dependence on AmI applications. Data losses can cause problems in personal relations, work discrimination, financial problems or even death, and recovering from some data losses can be impossible or require other than technological methods. Nevertheless, some problems can be solved by means of technology. For example, in event of theft of somebody's biometric data, there should exist means to replace compromised biometrics with another authentication method (other biometrics, tokens, etc) everywhere (in all credit cards, in all office/ home/ car locks, etc.), and to do it quickly and relatively effortlessly for the person, possibly via networks.

Another problem, which should be solved by technology means, is recovery from loss of or damage to a personal device. If a device is lost, personal data contained in it can be protected from strangers by diverse security measures, such as data encryption and strict access control. However, it is important that the user does not need to spend time customising and training a new device (so that denial of service does not happen). Instead, the new device should itself load user preferences, contacts, favourite music, etc from some back-up service, probably home server. We suggest that ways be developed to synchronise data in personal devices with a back-up server in a way that is secure and requires minimal effort by the user.

4.2.9 Conclusion

In the previous sections, technological safeguards for protecting user privacy in future ambient intelligence applications were proposed. We suggest that the most important, but not yet mature safeguards are the following:

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

[191] BBC News, "Huge surge in mobile phone thefts", 8 Jan 2002. http://news.bbc.co.uk/1/hi/uk/1748258.stm

- providing ways of disconnecting in such a way that nobody be sure why a user is not connected;
- increasing security by making software updates easier (automatically or semi-automatically, and at a convenient time for the user), detection of unusual patterns, improved encryption;
- increasing software intelligence by developing methods to detect and to hide sensitive data; to understand ethics and etiquette of different cultures; to speak different languages and to understand and translate human speech in many languages, including a capability to communicate with the blind and deaf;
- developing user-friendly means for recovery when security or privacy has been compromised.

4.3 SOCIO-ECONOMIC SAFEGUARDS

Apart from the safeguards targeted towards the individual citizen presented in this chapter, on a general level, effective distribution of organisational responsibilities and policy measures are needed as supporting measures as well. The responsibilities of different stakeholders in the implementation of AmI have to be defined in order to provide an effective and equitable decisional instrument for initiatives, priorities and measures. Since citizens and businesses obviously have different interests, governments but also industry associations, civil rights groups and other civil society organisations can play an important role in balancing these interests for the benefit of all affected groups.

Thus, co-operation between producers and users of AmI technology in all phases from R&D to deployment is essential to address some of the threats and vulnerabilities posed by AmI. The integration of or at least striking a fair balance between the interests of the public and private sectors will ensure more equity, interoperability and efficiency.

4.3.1 Balancing public and private interests

Co-operation between producers and users of AmI technology in all phases from R&D to deployment is essential to address some of the threats and vulnerabilities posed by AmI. The integration of or at least striking a fair balance between the interests of the public and private sectors will ensure more equity, interoperability and efficiency. Therefore, the most relevant safeguards respectively concern

- equitable distribution of resources, with a multi-stakeholder approach to building a people-centred, inclusive and development-oriented information society, as in the endorsement by the UN General Assembly of the outcomes of the World Summit for the Information Society (WSIS), which concluded in Tunisia in November 2005,[192].
- technical regulations,
- information security.

[192] http://www.un.org/News/Press/docs/2006/ga10451.doc.htm. See also Tokyo Ubiquitous Network Conference, Chairman's Report, 2005. www.itu.int/itu-wsis/2005/D-23chairmans_report.pdf

4.3.2 Standards

Standards form an important safeguard in many domains, not least of which are those relating to privacy and information security. Organisations should be expected to comply with standards, and standards-setting initiatives are generally worthy of support.

While there have been many definitions and analyses of the dimensions of privacy, few of them have become officially accepted at the international level, especially by the International Organization for Standardization. The ISO has at least achieved consensus on four components of privacy, as follows:
Anonymity ensures that a subject may use a resource or service without disclosing its user identity.
Pseudonymity ensures that a user may use a resource or service without disclosing its identity, but can still be accountable for that use.
Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.[193]

Among the ISO standards relevant to privacy and, in particular, information security are ISO/IEC 15408 on evaluation criteria for IT security and ISO 17799, the Code of practice for information security management, details of which are discussed in the following section.

The ISO has also established a Privacy Technology Study Group (PTSG) under Joint Technical Committee 1 (JTC1) to examine the need for developing a privacy technology standard. This is an important initiative and merits support. Its work and progress should be tracked closely by the EC, Member States, industry and so on.

Among the inputs to the ISO JTC 1 work on privacy is that developed by the International Security, Trust, and Privacy Alliance (ISTPA), a global alliance of companies, institutions and technology providers who are working together to clarify and resolve existing and evolving issues related to security, trust and privacy.[194] With the support of two of its members, ISTPA has provided ISO with a draft international standard (ISO/IEC (PAS) DIS 20886) for a privacy framework. According to the ISTPA, the framework provides an analytical starting point and basis for developing products and services that support current and evolving privacy regulations and business policies, both international and domestic.

A somewhat similar initiative is that of the PETTEP (Privacy Enhancing Technology Testing and Evaluation Project; see www.ipc.on.ca), an international venture to build a certification infrastructure for privacy systems. Its approach is somewhat like that of the Common Criteria in that it defines "profiles" as testable requirements for data security, privacy-protecting data management and accountability. Its goal is to provide assurance that systems making privacy-related claims actually perform as specified.

[193] ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*, First edition, International Organization for Standardization, Geneva, 1999. The standard is also known as the Common Criteria.
[194] http://www.istpa.org

4.3.3 ISO 17799 guidelines for information security

In 2000, the ISO published its standard ISO 17799 ("Code of practice for information security management"), which was updated in July 2005. Since then, an increasing number of organisations worldwide formulate their security management systems according to this standard. It provides a set of recommendations for information security management, focusing on the protection of information as an asset. It adopts a broad perspective that covers most aspects of information systems security.[195]

Among its recommendations for organisational security, ISO 17999 states that "the use of personal or privately owned information processing facilities ... for processing business information, may introduce new vulnerabilities and necessary controls should be identified and implemented."[196] By implementing such controls, organisations can, at the same time, achieve a measure of both organisational security and personal data protection. It also suggests that an appropriate set of procedures should be defined for information labelling and handling, in accordance with the classification scheme adopted by the organisation. These procedures should cover information assets in both physical and electronic formats, as well as different activities, such as copying, storage and transmission. To provide for the employees' privacy, organisations complying with the ISO 17799 should adapt their classification scheme according to the monitoring and privacy protection guidelines.

To reduce the risks stemming from human errors, theft, fraud or misuse of facilities, ISO 17799 proposes a wide set of security controls, including that the employees' legal responsibilities and rights, e.g., those stemming from data protection legislation, should be clarified and included within the terms and conditions of employment.

The standard also states explicitly the importance of user awareness, and proposes a set of recommendations "To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities".[197] Especially according to the principle of transparency, employees must be aware of all monitoring practices, along with the reasons for the monitoring. Since, in most cases, workplace monitoring is used to address inside security breaches, it is evident that including the issues of workplace surveillance in a security training and awareness program can help avoid negative employee attitudes and, at the same time, promote security awareness among employees. Moreover, the standard suggests that a formal disciplinary process should be in place for employees who have violated organisational security policies and procedures.

The standard suggests that consideration should be given to the security and business implications of the use of information and communication systems. To address problems that can arise from their use, ISO 17799 suggests that appropriate policies and guidelines should be prepared and implemented to confront issues such as:

---

[195] Similar standards and guidelines have also been published by other EU Member States: The British standard BS7799 was the basis for the ISO standard. Another prominent example is the German IT Security Handbook (BSI 1992).

[196] ISO/IEC 17799:2005(E), *Information Technology – Security techniques – Code of Practice for Information Security Management*, International Organization for Standardization, Geneva, 2005, p. 11

[197] ISO/IEC 17799:2005, p.25

1. vulnerabilities of information in information systems, e.g., automatic access to information in personal devices or via ad-hoc networking in the case of ambient intelligence,
2. policy and appropriate controls to manage information sharing,
3. categories of staff, contractors or business partners allowed to use the system and the locations from which it may be accessed. [198]

Additionally, the standard also suggests that, with regard to systems that are publicly available, security controls should be implemented so that "information is obtained in compliance with any data protection legislation" and especially "sensitive information will be protected during collection, processing, and storage".[199]

Finally, ISO 17799 suggests that compliance with data protection legislation is best achieved by the appointment of a data protection officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed.

ISO 17799 acknowledges the importance of legislative requirements, such as legislation on data protection and privacy of personal information and on intellectual property rights, for providing a "good starting point for implementing information security".[200] According to the standard, an essential part of any information security management system is a security policy aiming to "provide management direction and support for information security".[201] The standard also requires that the security policy includes "a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization"[202], especially those that concern compliance with legislative and contractual requirements. In this way, an organisation applying a security policy can inform its employees about the data protection and privacy legislation with which the organisation complies.

It also suggests that, besides applying an organisation-wide information security policy, effective security management requires that more detailed security policies and procedures for specific information systems or security rules should also be formulated for day-to-day use of information and communication systems.

Such an operational policy can provide a common basis of understanding of for what and how employees can use information and communication systems. A well written and carefully worded policy that informs employees on the tools and methods for collecting data, and the purpose of the collection, are more likely to avoid hostile employee reaction and gain employee tolerance or even support. ISO 17799 acknowledges that "the co-operation of authorized users is essential for effective security".[203] Although the formulation of an operational policy is dependent on the technological as well as the organisational context, several aspects of use policies are common in most organisations.

[198] ISO/IEC 17799:2005, p. 52
[199] ISO/IEC 17799:2005, p. 55.
[200] ISO/IEC 17799:2005, p. ix.
[201] ISO/IEC 17799:2005, p. 7.
[202] ISO/IEC 17799:2005, p. 7.
[203] ISO/IEC 17799:2005, p. 63.

The following list of key points, based on an analysis of legal, organisational and security issues, could help organisations to develop policies that are lawful and fair and that promote security:

- The use policy should state its scope.
- The use policy should be compliant with data protection legislation.
- It should contain clear guidelines as to how employees may and may not use electronic means of communication.
- The use policy should state the purposes for which data collecting and monitoring is conducted.
- The use policy should describe the methods and tools applied for monitoring.
- The disciplinary process in case the policy is violated should be defined.
- The use policy should describe the alternatives employees can use to preserve the confidentiality of communications.
- Automated tools and systems should be used for scanning electronic communication flow including protection against viruses and other types of malicious code.
- The policy should inform employees who is responsible for overseeing its application.
- The policy should also refer to scheduled reviews and modification procedures.

ISO 17799 is an important standard, but it could be described more as a framework than a standard addressing specificities of appropriate technologies or how those technologies should function or be used. Also, ISO 17799 was constructed against the backdrop of today's technologies, rather than with AmI in mind. Hence, the adequacy of this standard in an AmI world needs to be considered. Nevertheless, organisations should state to what extent they are compliant with ISO 17799 and/or how they have implemented the standard.

4.3.4 Audits

Audit logs may not protect privacy since they are aimed at determining whether a security breach has occurred and, if so, who might have been responsible or, at least, what went wrong. The ISO 17799 standard recommends that audit logs should be kept that would identify
a) user IDs;
b) dates, times, and details of key events, e.g., log-on and log-off;
c) terminal identity or location if possible;
d) records of successful and rejected system access attempts;
e) records of successful and rejected data and other resource access attempts;
f) changes to system configuration;
g) use of privileges;
h) use of system utilities and applications;
i) files accessed and the kind of access;
j) network addresses and protocols;
k) alarms raised by the access control system;
l) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

Audit logs could have a deterrent value in protecting privacy and certainly they could be useful in prosecuting those who break into systems without authorisation. The requirement for independent audits has featured in some recent court decisions.

- After a data breach in 2005 at Atlanta-based CardSystems that left some 40 million customer accounts vulnerable to hackers, the company's new owners (CardSystems' assets were bought by San Francisco-based Pay By Touch) are obliged to implement a comprehensive security program and obtain independent audits every other year for 20 years.[204]
- Similarly, Sony agreed to an independent audit of its uses of digital rights management software over two years to ensure that its privacy practices are fair to consumers.[205]

In the highly networked environment of our AmI future, maintaining audit logs will be a much bigger task than now where discrete systems can be audited. Nevertheless, those designing AmI networks should ensure that the networks have features that enable effective audits.

4.3.5 Open standards

The dominance of a small number of hardware and software suppliers with a proprietary system architecture can have severe negative effects not only on competition but also on the security of ICT systems and the confidence that users have in the technology and its producers. The frequent attacks on Microsoft systems give clear evidence of this fact. These risks, however, can be minimised by giving preference to open, product-independent standards.

Open systems are considered by many experts as the only way to achieve two important goals: interoperability and competition.[206] Interoperability means that independently developed systems or components can connect to each other, exchange information and operate in tandem without loss of functionality. Because of the complexity and diversity of the components that make up an AmI network, interoperability is one of its biggest technical challenges. The research and business community will take any technique seriously if it can increase interoperability.

Openness as a standard restructures the market for networking products by defining competitiveness as being able to include, rather than exclude, other vendors' products. Open systems promise to open markets for smaller vendors, eliminating the competitive advantage of having a large installed base. Obviously this idea is less appealing to vendors who already control a large share of the market. For users, openness holds out the promise of greater choice and ease of use. Openness implies standardisation and simplicity of operation. Openness is also supposed to give consumers the ability to choose products based on price or performance rather than compatibility and to protect them from being dependent on a single source.

Apart from the positive effects of open innovations as such, we would support the development of protection software (against viruses, spam, spyware, etc.) under the open source development model. Though open source is no panacea for security problems, there is evidence that open source software can lead to robust and reliable products. But, as

[204] Kerr, Jennifer C., "Credit Card Payment Co. Settles Charges", Associated Press, 23 Feb 2006.
[205] "Sony BMG to settle 'rootkit' lawsuits", *OUT-LAW News*, 4 Jan 2006.
http://www.out-law.com/page-6496
[206] Simon, K. D., "The Value of Open Standards and Open-Source Software in Government Environments", *IBM Systems Journal*, vol.44, no. 2, 2005, pp. 227-38; Alvestrand, H., "The Role of the Standards Process in Shaping the Internet", *Proceedings of the IEEE*, vol. 92, no. 9, 2004, pp. 1371-74.

Hansen et al. state: "No single state can finance this development alone."[207] In addition, open source software could raise other issues, such as liability.

Thus, promoting open systems and open standards at a European level is a good attempt at building a system that could be more trustworthy, to mediate between public and private control over networked systems and will therefore contribute to security and privacy in AmI.[208]

4.3.6 Codes of practice

The OECD has been working on privacy and security issues for many years. It produced its first guidelines more than 25 years ago. Its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[209] were (are) intended to harmonise national privacy legislation. The guidelines were produced in the form of a Recommendation by the Council of the OECD and became applicable in September 1980. The guidelines are still relevant today and may be relevant in an AmI world too, but it has been argued that they may no longer be feasible in an AmI world.[210]

The OECD's more recent Guidelines for the Security of Information Systems and Networks are also an important reference in the context of developing privacy and security safeguards. These guidelines were adopted as a Recommendation of the OECD Council (in July 2002). In December 2005, it published a report on "The Promotion of a Culture of Security for Information Systems and Networks", which it describes as a major information resource on governments' effective efforts to date to foster a shift in culture as called for in the aforementioned Guidelines for the Security of Information Systems and Networks.

In November 2003, the OECD published a 392-page volume entitled Privacy Online: OECD Guidance on Policy and Practice, which contains specific policy and practical guidance to assist governments, businesses and individuals in promoting privacy protection online at national and international levels.

In addition to these, the OECD has produced reports on other privacy-related issues including RFIDs, biometrics, spam and authentication.[211]

Sensible advice can also be found in a report published by the US National Academies Press in 2003, which said that to best protect privacy, identifiable information should be collected only when critical to the relationship or transaction that is being authenticated.

---

[207] Hansen, M., K. Köhntopp and A. Pfitzmann, "The Open Source Approach - Opportunities and Limitations with Respect to Security and Privacy", *Computers and Security*, vol. 21, no. 5, 2002, pp. 461-71. See also Payne, C., "On the Security of Open Source Software", *Information Systems Journal*, vol. 12, no. 1, 2002, pp. 61-78.

[208] Kravitz, D. W., K.-E. Yeoh and N. So, "Secure Open Systems for Protecting Privacy and Digital Services", in T. Sander (ed.), *Security and Privacy in Digital Rights Management,* ACM CCS-8 Workshop DRM 2001, Philadelphia, 5 Nov 2001, Revised Papers, Springer, Berlin, 2002, pp. 106 – 25; Gehring, R. A., "Software Development, Intellectual Property, and IT Security", *The Journal of Information, Law and Technology*, 1/2003. http://elj.warwick.ac.uk/jilt/03-1/gehring.html.

[209] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[210] See Čas, Johann, "Privacy in Pervasive Computing Environments – A Contradiction in Terms?", *Technology and Society Magazine*, IEEE, Volume 24, Issue 1, Spring 2005, pp. 24-33.

[211] http://www.oecd.org/department/0,2688,en_2649_34255_1_1_1_1_1,00.html

The individual should consent to the collection, and the minimum amount of identifiable information should be collected and retained. The relevance, accuracy and timeliness of the identifier should be maintained and, when necessary, updated. Restrictions on secondary uses of the identifier are important in order to safeguard the privacy of the individual and to preserve the security of the authentication system. The individual should have clear rights to access information about how data are protected and used by the authentication system and the individual should have the right to challenge, correct, and amend any information related to the identifier or its uses.[212]

Among privacy projects, PRIME has identified a set of privacy principles in the design of identity management architecture.
Principle 1: Design must start from maximum privacy.
Principle 2: Explicit privacy rules govern system usage.
Principle 3: Privacy rules must be enforced, not just stated.
Principle 4: Privacy enforcement must be trustworthy.
Principle 5: Users need easy and intuitive abstractions of privacy.
Principle 6: Privacy needs an integrated approach.
Principle 7: Privacy must be integrated with applications.[213]

Other guidelines were referenced in the first SWAMI report.

4.3.7 Trust marks and trust seals

Trust marks and trust seals can also be useful safeguards because the creation of public credibility is a good way for organisations to alert consumers and other individuals to an organisation's practices and procedures through participation in a program that has an easy-to-recognise symbol or seal. An example of a European trustmark is the CCT mark, developed by the UK government. CCT is the abbreviation for CSIA Claims Tested (CCT), which is used to indicate that security software meets government standards.[214] CSIA is the Central Sponsor for Information Assurance, a new Cabinet Office unit that works with partners in the public and private sectors, as well as its international counterparts, to help safeguard the nation's IT and telecommunications services. Examples of other trust seal systems are TrustUK, L@belsite (France), Trustedshops (Germany) and Japan DMA; the Global Trustmark Alliance promotes the use of quality seals at an international level.

Trust marks and seals are a form of guarantee provided by an independent organisation that maintains a list of trustworthy companies that have been audited and certified for compliance with some industry-wide accepted or standardised best practice in collecting personal or sensitive data. Once these conditions are met, they are allowed to display a trust seal logo or label that customers can easily recognise.[215]

---

[212] Kent, Stephen T., and Lynette I. Millett (eds.), *Who Goes There?: Authentication Through the Lens of Privacy*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academies Press, Washington, DC, 2003, Chapter 3.
[213] For more details about each principle, see Sommer, Dieter, Architecture Version 0, PRIME Deliverable D14.2.a, 13 October 2004, pp. 35-6 and pp. 57-58. www.prime-project.eu.org
[214] "UK gov flies IT security kitemark", OUT-LAW.COM, 9 Sept 2005.
[215] Pennington, R., H. D. Wilcox and V. Grover, "The Role of System Trust in Business-to-Consumer Transactions", *Journal of Management Information System*, vol. 20, no. 3, 2004, pp. 197-226; Subirana, B., and M. Bain, *Legal Programming: Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond*, Springer, New York, 2005.

Such a trust mark must implement mechanisms necessary to maintain objectivity and build legitimacy with consumers. It should utilise a governing structure that solicits and considers input from the business community, consumer/advocacy organisations and other stakeholders and experts in formulating its policies. Trust marks should strive to create a consistent and predictable framework in implementing its procedures. The trust mark program should be independent, comprehensive and accessible. It should endeavour to make receipt of the seal affordable for and available to all parties especially small and medium-size businesses.

Trust seals and trust marks are, however, voluntary efforts that are not legally binding and an effective enforcement needs carefully designed procedures and the backing of an independent and powerful organisation that has the confidence of all affected parties. To this end, a trust mark requires:

- **Verification and monitoring:** Validation and monitoring by an independent trusted third party that organisations are engaged in meaningful self-regulation of online privacy may be necessary to grow consumer confidence. The validation can either be a self-assessment or a compliance review prior to awarding the trust mark. If a self-assessment is chosen, it must be pursuant to a rigorous, uniform, clearly articulated and publicly disclosed methodology under which an organisation would be asked to verify that its published privacy and/or security policy is accurate, comprehensive, prominently displayed, completely implemented and accessible; and that consumers are informed of the complaint resolution mechanisms. Such a self-assessment must be reviewed by the trust mark provider to ensure compliance with the methodology. Periodic reviews should be required by the trust mark provider to ensure that those displaying the trust mark continue to abide by their policies and that those policies continue to be consistent with its principles. In cases where there is evidence that a company is not abiding by its policies, the trust mark provider should establish clear criteria for placing that company on probation or beginning procedures for the seal's revocation. The provider should establish clearly defined criteria for when and how a company's seal may be revoked. Seal revocation should be a matter of public record. The provider must clearly state the grounds for revocation and establish a post-revocation appeals process.
- **Conflict resolution:** An effective enforcement mechanism must also provide a mechanism to resolve conflicts and consequences for failure to do so. Thus, a trust mark provider must define a system for addressing conflicts and provide staff to resolve them. However, the conflict resolution mechanisms should only be applied when a conflict cannot adequately be resolved between the complaining consumer and the company. Conflict resolution outcomes must not be contrary to any existing legal obligations of the participating company. Failure of a company to agree with the outcome of the conflict resolution process should result in previously identified consequences to the company. Notwithstanding the conflict resolution process, the consumer, the company and the trust mark provider may pursue other available legal recourse.
- **Education and outreach:** A trust mark program must develop and implement policies to educate consumers and business about online privacy and implement policies to encourage awareness of the program and privacy and security issues with both

consumers and businesses. This may include: publicity for participating companies, public disclosure of material non-compliance or seal revocation, periodic publication of the results of the monitoring and review procedures, or referral of non-complying companies to the appropriate government agencies.

Several private sector groups have been formed to monitor industry's attempts at establishing privacy protections. Examples include TRUSTe[216], BBBOnline[217], CPA WebTrust[218] and the OPA (Online Privacy Alliance)[219].

These groups are often composed of industry, as opposed to consumer-interest, groups. As a result, concerns exist that consumers' desires for stringent privacy protections may be compromised in the interest of industry's desire for the new currency of information. Moreover, empirical evidence indicates that even some eight years after the introduction of the first trust marks and trust seals in Internet commerce, citizens know little about them and none of the existing seals has reached a high degree of familiarity among customers.[220] Though this does not necessarily mean that trust marks are not an adequate safeguard for improving the security and privacy in the ambient intelligence world, it suggests that voluntary activities like self-regulation have – apart from being well designed – to be complemented by other legally enforceable measures.[221]

4.3.8 Reputation systems and trust-enhancing mechanisms

It has previously been pointed out (cf. section 2.4) that trust – in addition to the general influence cultural factors and socialisation exert – results from context-specific interaction experiences. The importance of trust rests in its function to reduce social complexity and uncertainty. Without a minimum level of trust, interactions with the social environment cannot take place. As is well documented, computer-mediated interactions are different from conventional face-to-face exchanges due to anonymity, lack of social and cultural clues, 'thin' information, and the uncertainty about the credibility and reliability of the provided information that commonly characterise mediated relationships.[222]

In an attempt to reduce some of the uncertainties associated with online commerce, many websites acting as intermediaries between transaction partners are operating so-called reputation systems. These institutionalised feedback mechanisms are usually based on the

[216] The TRUSTe program (http://www.truste.org) was released in 1997 by a consortium of CommerceNet, the Electronic Frontier Foundation (EFF) and the Boston Consulting Group as an independent, non-profit organisation.
[217] BBBOnline (http://www.bbbonline.org) was released in 1999, by the Better Business Bureau (BBB). BBB is an independent US business service "dedicated to fostering fair and honest relationships between businesses and consumers, instilling consumer confidence and contributing to an ethical business environment".
[218] CPA WebTrust (http://www.cpawebtrust.org) was released in 1997 by the American Institute of Certified Public Accountants.
[219] http://www.privacyalliance.org
[220] Moores, T., "Do Consumers Understand the Role of Privacy Seals in E-Commerce?", *Communications of the ACM*, Vol. 48, no. 3, 2005, pp. 86-91.
[221] Prins, J. E. J., and M.H.M. Schellekens, "Fighting Untrustworthy Internet Content: In Search of Regulatory Scenarios", *Information Polity*, vol.10, 2005, pp. 129-39.
[222] For an overview over the vast literature on the topic, cf. Burnett, R. and P.D. Marshall, *Web Theory: An Introduction*, Routledge, London 2002, pp. 45-80.

disclosure of past transactions rated by the respective partners involved.[223] Making the history of past interactions public is intended to inform potential partners about the credibility and trustworthiness of the hitherto unknown other party. Moreover, giving participants the opportunity to rank their counterparts creates an incentive for rule-abiding behaviour. Robert Axelrod aptly phrased the expectation of reciprocity in future interactions as the "shadow of the future"[224]. Thus, reputation systems seek to imitate some of the real-life trust-building and social constraint mechanisms in the context of mediated interactions.

Web-based auctioneers such as eBay[225] initially popularised reputation systems. Since then, many other intermediaries offer ratings for a plethora of online markets and computer-mediated interactions. Customers may evaluate retailers at Bizrate[226] or at Shopping.com[227], and on so-called expert sites such as AskMe[228] or ExpertCentral[229], expert advice is given in exchange for reputation points. In the area of specialised forums and news sites, Slashdot[230] has incorporated a ranking system as well. Many social software applications (e.g., Flickr[231] or Del.icio.us[232]) not only use the feedback mechanisms but also creatively combine them with additional opportunities for cross-referencing, personal comments and content, thereby contributing to the development of multifaceted, dense relationships. Moreover, in a growing number of services such as OpenBC[233] or Linked-In[234], the conventional anonymity of web-based social networks – based on nicknames and aliases – is being replaced by the disclosure of the participants' offline identities as an attempt to build trust.[235]

So far, reputation systems have not been developed for AmI services. And it seems clear that institutionalised feedback mechanisms will only be applicable to a subset of future AmI services and systems. Implementing reputation systems only makes sense in those cases in which users have real choices between different suppliers (for instance, with regard to AmI-assisted commercial transactions or information brokers). AmI infrastructures which normally cannot be avoided if one wants to take advantage of a service, need to be safeguarded by other means, such as trust seals, ISO guidelines and regulatory action.

Despite quite encouraging experiences in numerous online arenas, reputation systems are far from perfect. Generally, it should be kept in mind that many reputation systems tend to shift the burden of quality control and assessment from professionals to the – not

[223] Resnick, P. and R. Zeckhauser, "Trust Among Strangers in Internet Transactions: Empircal Analysis of eBay's Reputation System", in Michael R. Baye (ed.), *The Economics of the Internet and E-Commerce*, Vol. 11 of Advances in Applied Microeconomics, JAI Press, Amsterdam, 2002, pp. 127-157; Vishwanath, A., "Manifestations of Interpersonal Trust in Online Interaction", *New Media and Society*, Vol. 6 (2), 2004, pp. 224 f.
[224] Axelrod, R., *The Evolution of Cooperation*, Basic Books, New York, 1985.
[225] http://www.ebay.com
[226] http://www.bizrate.com
[227] http://www.shopping.com
[228] http://www.askmecorp.com
[229] http://www.expertcentral.com
[230] http://slashdot.org
[231] http://www.flickr.com
[232] http://del.icio.us
[233] http://www.openbc.com
[234] https://www.linkedin.com
[235] Sixtus, M., "Das Web sind wir", *Technology Review*, Heft 3, July 2005, pp. 44-52.

necessarily entirely informed – individual user. In consequence, particularly sensitive services should not exclusively be controlled by voluntary and market-style feedbacks from customers. Furthermore, reputation systems are vulnerable to manipulation. Pseudonyms can be changed, effectively erasing previous feedback. And the feedbacks themselves need not necessarily be sincere, either due to co-ordinated accumulation of positive feedbacks, due to negotiations between parties prior to the actual feedback process, because of blackmailing or the fear of retaliation.[236] Last not least, reputation systems can become the target of malicious attacks, just like any net-based system.

An alternative to peer-rating systems are credibility-rating systems based on the assessment of trusted and independent institutions, such as library associations, consumer groups or other professional associations with widely acknowledged expertise within their respective domains. Ratings would be based on systematic assessments along clearly defined quality standards. In effect, these variants of reputation- and credibility-enhancing systems are quite similar to trust marks and trust seals (see previous section). The main difference is that professional rating systems enjoy a greater degree of independence from vested interests. And, other than in the case of peer-rating systems which operate literally for free, the independent professional organisations need to be equipped with adequate resources.

On balance, reputation systems can contribute to trust-building between strangers in mediated short-term relations or between users and suppliers, but they should not be viewed as a universal remedy for the ubiquitous problem of uncertainty and the lack of trust. Moreover, feedback systems need to be integrated in and combined with other AmI safeguards, such as education, regulation and security, to name just a few. Additional research from different angles, including psychology, sociology and cultural studies, is expedient in order to address the numerous challenges associated with reputation systems in general and in AmI environments in particular.

4.3.9 Service contracts

A possible safeguard is a contract between the service provider and the user that has provisions about privacy rights and the protection of personal data and notification of the user of any processing or transfer of such data to third parties. While this is a possible safeguard, there must be some serious doubt about the negotiating position of the user. It's quite possible the service provider would simply say here are the terms under which I'm willing to provide the service, take it or leave it. Also, from the service provider's point of view, it's unlikely that he would want to conclude separate contracts with every single user.

In a world of ambient intelligence, such a prospect becomes even more unlikely in view of the fact that the "user", the consumer-citizen will be moving through different spaces where there is likely to be a multiplicity of different service providers. It may be that the consumer-citizen would have a digital assistant that would inform him of the terms, including the privacy implications, of using a particular service in a particular environment. If the consumer-citizen did not like the terms, he wouldn't have to use the service.

[236] Resnick, P., R. Zeckhauser, E. Friedman and K. Kuwabara,. "Reputation Systems: Facilitating Trust in Internet Interactions", *Communications of the ACM*, 43(12), 2000, pp. 45-48. http://www.si.umich.edu/~presnick/papers/cacm00/reputations.pdf (retrieved: 11 April 2006).

Consumer associations and other civil society organisations (CSOs) could, however, play a useful role as a mediator between service providers and individual consumers and, more particularly, in forcing the development of service contracts (whether real or implicit) between the service provider and the individual consumer. Consumer organisations could leverage their negotiating position through the use of the media or other means of communication with their members. CSOs could position themselves closer to the industry vanguard represented in platforms such as ARTEMIS by becoming members of such platforms themselves. Within these platforms, CSOs could encourage industry to develop "best practices" in terms of provision of services to consumers.

4.3.10 Guidelines for ICT research

Government support for new technologies should be linked more closely to an assessment of technological consequences. On the basis of the far-reaching social effects that ambient intelligence is supposed to have and the high dynamics of the development, there is a clear deficit in this area.[237] Research and development (at least publicly supported R&D) must highlight future opportunities and possible risks to society and introduce them into public discourse. Every research project should commit itself to explore possible risks in terms of privacy, security and trust, develop a strategy to cover problematic issues and involve users in this process as early as possible.

A template for "design guidelines" that are specifically addressing issues of privacy has been developed by the "Ambient Agora" project[238] which has taken into account the fundamental rules by the OECD, notably its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted on 23 September 1980 and the more recent *Guidelines for the Security of Information Systems and Networks*.[239] The guidelines make the point that privacy enhancement is better obtained by actively constructing a system exactly tailored to specific goals than by trying to defend ex-post a poor design against misuse or attacks. The nine guidelines are as follows: [240]

1. *Think before doing:* Evaluate potential system impacts. The very nature of a system or its parts may be against privacy in their intention.
2. *Re-visit classic solutions:* Search for existing solutions in the physical world or in old systems for the similar class of problem/service, and understand the way in which new technologies change the effects of classic issues.

[237] Langheinrich, M., "The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects", Paper presented at the Designing for Privacy Workshop, DC Tales Conference, Santorini, Greece, 2003.
[238] Lahlou, S., and F. Jegou, "European Disappearing Computer Privacy Design Guideslines V1", Ambient Agora Deliverable D15.4, Electricité de France, Clamart, 2003. http://www.ambient-agoras.org/downloads/D15[1].4_-_Privacy_Design_Guidelines.pdf. The guidelines were subsequently and slightly modified and can be found at http://www.rufae.org/privacy. See also Langheinrich, M., "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems", in G. D. Abowd, B. Brumitt and S. A. Shafer (eds.), *Proceedings of the Third International Conference on Ubiquitous Computing* (Ubicomp 2001), Springer-Verlag, Berlin, 2001, pp. 273-91.
[239] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Co-operation and Development, Paris, 2001; *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Organisation for Economic Co-operation and Development, Paris, 2002.
[240] Lalou and Segou, 2003.

3. *Openness:* Systems should give human users access to what they do, do it, and do nothing else. Help human users construct a valid and simple mental model of what the system does. Goals, ownership and state of system should be explicit, true and easily accessible to human users, in a simple format.
4. *Privacy razor:* Human user characteristics seen by the system should contain *only* elements, which are necessary for the explicit goal of the activity performed with the system. No data should be copied without necessity.
5. *Third party guarantee:* Using a neutral or trusted third party may open more solutions or lighter design. It may enable entitlement, validation, control, claim, archive, etc. without direct data transfer between system and subject. In case of third party involvement, give the user choice.
6. *Make risky operations expensive:* No system is 100 % privacy safe. Subjects should be made aware of which operations are privacy-sensitive. Operations identified as privacy-sensitive should be made costly for the system, the human user and the third party.
7. *Avoid surprise:* Human users should be made aware when their activity has an effect on the system. Acknowledgement should be explicit for irreversible major changes. Cancellation should be an option as much as possible, not only in the interface, but also in the whole interaction with the system.
8. *Consider time:* Expiry date should be the default option for all data.
9. *Good privacy is not enough:* Safety, security, sustainability, equity … are important issues with which trade-offs may have to be considered. These trade-offs should be discussed with stakeholders or their representatives as much as possible.

4.3.11 Public procurement

If the state acts as a buyer of strategically important innovative products and services, it contributes to the creation of the critical demand that enables suppliers to reduce their business risk and realise spill-over effects. Thus, public procurement programs can be used to support the demand for and use of improved products and services in terms of security and privacy or identity protection.

In the procurement of ICT products, emphasis should therefore be given to critical issues such as security and trustworthiness. As in other advanced fields, it will be a major challenge to develop a sustainable procurement policy that can cope with ever-decreasing innovation cycles. The focus should not be on the characteristics of an individual product or component, but on the systems into which components are integrated.

Moreover, it is important to pay attention to the secondary and tertiary impacts resulting from deployment of *large technical systems* such as ambient intelligence. An evaluation of the indirect impacts is especially recommended for larger (infrastructure) investments and public services.

While public procurement of products and services that are compliant with the EU legal framework and other important guidelines for security, privacy and identity protection is no safeguard on its own, it can be an effective means for the establishment and deployment of standards and improved technological solutions.[241]

[241] See for instance Edler, J., (ed.), "Politikbenchmarking Nachfrageorientierte Innovationspolitik", Progress report No. 99, Office for Technology Assessment at the German Parliament, Berlin, 2006; Molas-Gallart, J.,

4.3.12 Accessibility and social inclusion

For the purpose of this study, accessibility is viewed as a key concept helping to promote the social inclusion of all citizens in the information society with the use of AmI technologies. We do not focus on specific groups, people with disabilities and older persons, i.e., people with difficulties in accessing these new technologies and services. In this study, accessibility is needed to ensure user control, acceptance and enforceability of policy in a user-friendly manner, with a view to support accessibility and the provision of citizens with real equal rights and opportunities in a world of ambient intelligence.

This point may embrace four safeguards (or principles) relating to:

- equal rights and opportunities
- usability (vs. complexity)
- training
- dependability.

The table below links each identified threat and vulnerability regarding digital divide (vertical axis) with the corresponding safeguards (horizontal axis) that have been identified to address them. More details of each safeguard is made in the paragraphs that follow and elsewhere in this chapter.

Threats and vulnerabilities \ Safeguards			Standards	Interoperability/harmonisation	Accessibility/ Social Inclusion				Effective distribution of organisational responsibilities and policy measures	Convergence of public and private interests			Accountability
					Equal rights and opportunities	**Usability**	**Training**	**Dependability**		**Equitable distribution of resources**	**Technical regulations**	**Enhancing information security**	
Dependency	**Technological dependency**	**Insufficient interoperability (*Spatial aspect*)**	✓	✓				✓		✓	✓		
		Insufficient interoperability (*Temporal aspect*)		✓				✓			✓		
		High update and maintenance costs		✓					✓	✓	✓		
	User dependency	**Systems take control**			✓	✓		✓			✓		
		"AmI technosis"					✓	✓					
		Stress				✓	✓				✓		
		Unsafe usage (due to lack of rules)					✓				✓		
Exclusion		**Unequal access**			✓					✓			

"Government Policies and Complex Product Systems: The Case of Defence Standards and Procurement", *International Journal of Aerospace Management*, vol. 1, no. 3, 2001, pp. 268-80.

/discrimination	**Stigmatisation / Profiling**										✓	✓
	Victimisation			✓							✓	✓
	Voluntary exclusion					✓						✓

Equal rights and opportunities

All citizens should have equal rights to benefit from the new opportunities that AmI technologies will offer. This policy will promote the removal of direct and indirect discrimination, will foster access to services and encourage targeted actions in favour of under-represented groups.

Usability (vs. complexity of use)

This point will promote system design according to a user-centric approach (=the concept of "design for all"). The design-for-all concept enables all to use applications (speech technology for the blind, pictures for the deaf). It also means designing in a way that applications are user-friendly and can be used intuitively. In short, industry has to make an effort to simplify the usage of ICT, rather than prospective users being forced to learn how to use otherwise complex ICTs.

Better usability will then support easy learning (i.e., learning by observation), user control and efficiency, thus increasing satisfaction and, consequently, user acceptance.

This safeguard fights directly against user dependency and more particularly against user isolation and stress due to the complexity of new technology, which leads to loss of control.

Training

This action will promote education programs on learning how to use new technologies and will increase the user awareness about the different possibilities and choices offered by AmI technologies and devices. This safeguard is useful to deter different facets of user dependency, specially the facets associated with social disruption. User awareness is also important to reduce the voluntary exclusion caused by a misunderstanding on how the technology works.

Dependability

This safeguard is essential in order to prevent almost all facets of dependency, system dependency as well as user dependency, as defined in section 3.6.1 above. Indeed, the dependability challenges should be addressed by an effective implementation of AmI technologies by taking into account both technical constraints and harmonised human-machine interfaces.

- Technical constraints are, for example, the scale and pervasiveness of applications and services, the volume or number of components, heterogeneity of technologies and diversity of life cycles, intelligence and autonomy. Thus, interoperability among devices in spatial (e.g, by taking into account the volume, the heterogeneity) and temporal (e.g., by taking into account life cycle) ways will help to reduce technological dependency.

- Harmonised human-machine interfaces mainly encompass the compatibility between technology and human systems and technology-push with considerations in terms of social impact.[242] This second point focuses more on the human aspect of the dependency by promoting better integration (and the subsequent feeling of inclusion) of the user in AmI world, so reducing the mentioned problems (see part 3.6.1) such as system take-over or AmI technosis.

4.3.13 Raising public awareness

Consumers need to be educated about the privacy ramifications arising from virtually any transaction in which they are engaged. An education campaign should be targeted at different segments of the population. Targeting school-age children should be included in any such campaign.

Any networked device, particularly those used by consumer-citizens should come with a privacy warning much like the warnings on tobacco products.

Currently, when technology users start thinking about threats to privacy (if they make an effort to think about it), they evaluate privacy threats arising from some particular technologies taken separately from others. However, most users don't understand the dangers of information linkage: the fact that aggregation of data collected by several technologies simultaneously provides more information than several separate databases. It is necessary to educate users about this fact with well-selected examples.

From Scenario 3, second SWAMI report

Miles [*BBC reporter*]: *"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."*

If security has been lax at some companies, users must shoulder some responsibility, i.e., users must take a greater interest in how their data might be used or their communications violated.[243] They should look at privacy policies on websites and if those policies are too long and legalistic, they should ask for shorter, simpler policies written in plain English (or whatever language). They should look for trustmarks such as Trust-E. If they discover privacy policies have not been adhered to, they should complain not only to the company in question but also to industry watchdogs and to the government.

When the UK Department of Trade and Industry (DTI) released its 2004 information security review, Stephen Timms, the UK e-Commerce minister, emphasised that everyone

[242] There is a vast amount of activity on interfaces "for all". See, for example, Stephanidis, Constantine, et al, "Toward an Information Society for All: HCI Challenges and R&D Recommendations." *International Journal of Human-Computer Interaction* 11, no. 1, 1999, pp.: 1-28.

[243] Unfortunately, recent research indicates many consumers take few security precautions. A survey conducted for Lloyds TSB found that 40 per cent of users had not downloaded any security patches to fix security holes in Windows and other programs. Savvas, Antony, "Lax anti-virus practices fuel security fears", ComputerWeekly.com, 21 April 2005.

has a role to play in protecting information: "Risks are not well managed. We need to dispel the illusion the information security issues are somebody else's problem. It's time to roll up our sleeves."[244]

The OECD shares this point of view. It has said that "all participants in the new information society …need… a greater awareness and understanding of security issues and the need to develop a 'culture of security'."[245] The OECD uses the word "participants", which equates to "stakeholders", and virtually everyone is a participant or stakeholder – governments, businesses, other organisations and individual users. Its guidelines are aimed at promoting a culture of security, raising awareness and fostering greater confidence [=trust] among all participants. SWAMI strongly agrees with and supports the OECD guidelines. In fact, building on those guidelines, we go a step further, by recommending a more structured approach to promoting a culture of security, i.e., by initiating a risk assessment / risk management process involving all stakeholders (see the next chapter).

There are various ways of raising awareness, and one of those ways would be to have some contest or competition for the best security or privacy-enhancing product or service of the year. Such a contest or competition could be regarded like the UK's Booker Prize or the Oscars. The US government's Department of Homeland Security is sponsoring such competitions,[246] and Europe could usefully draw on their experience to hold similar competitions in Europe. We would suggest such competitions at Member State level and then at European level on an annual basis. Such competitions would serve to raise awareness as well as stimulating ever-more creative solutions to the key problems of security and privacy.

There is also a need for other awareness-raising initiatives for the general public. The Dutch Department of Financial Affairs has initiated an awareness-raising campaign for children, SurfopSafe, and together with other partners, the Department develops training modules for primary schools. One innovation was a special edition of Donald Duck where Donald and his nephews surfed safely on the Internet.[247]

4.3.14 Education

A self-aware, critical and responsible approach to ICTs is the best protection against many risks that could arise in an ambient intelligence society. In terms of general education, this means that the priorities should not be the pointless learning of skills for dealing with ICTs, but the acquisition of meaningful knowledge and the development of a critical basic attitude.

In the same way as the principle that "not everything that you read in the newspapers is true" has long been part of general education, in the ICT age, awareness should generally be raised by organisations that are as close to the citizen as possible and trustworthy (i.e.,

[244] Leyden, John, "Hackers cost UK.biz billions", *The Register*, 28 April 2004. http://www.theregister.co.uk/2004/04/28/dti_security_survey/

[245] *OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security*, OECD, Paris, 2002, p. 7.

[246] Lemos, Robert, "Cybersecurity contests go national", *The Register*, 5 June 2006. http://www.theregister.co.uk/2006/06/05/security_contests/
This article originally appeared at *SecurityFocus*. http://www.securityfocus.com/news/11394

[247] Swedish Emergency Management Agency (SEMA), *Society's Information Assurance: Status Assessment*; 2005, p. 23. http://www.krisberedskapsmyndigheten.se/6193.epibrw

on the local or regional level, national campaigns maybe co-ordinated by ENISA might help). Questions of privacy, identity and security are, or should be, an integral part of the professional education for computer scientists. Issues that should be part of such awareness include the following:

- possibilities and limits of digital content manipulation,
- the problem of assessing the authenticity and credibility of the originator of a piece of information,
- limits of the reliability of hardware-software systems, e.g., using the history of well-known computer errors,
- risks arising from the possibilities of criminal misuse of ICTs,
- impacts of ICTs on society, e.g., using historical developments since the invention of the computer,
- competition and market concentrations in the hardware, software and content markets,
- the differences between humans and machines, the possibilities and limits of machine intelligence,
- data privacy, information rights and security measures.

This content should, where possible, be integrated into existing school subjects, step by step. The focus should be on longer-term principles, and shorter-lived phenomena should be included only where they provide a clear example of a general principle. This measure requires several individual measures, including the incorporation of these issues into revised curricula and the further training of teaching staff.

Institutes of higher education should ensure that courses in ICT-relevant disciplines cover the following content:

- ICT and society: impacts of ICT on society,
- Knowledge from technology assessment (TA) or from 'impact and design research', which came into being in the field of computing,
- Promotion of awareness of development potential for health and the environment in the development phase of new technologies.

SWAMI agrees with and supports the Commission's recent "invitation" to Member States to "stimulate the development of network and information security programmes as part of higher education curricula".[248]

4.3.15 Media attention, bad publicity and public opinion

Perhaps one of the best safeguards is public opinion, stoked by stories in the press and the consequent bad publicity given to perceived invasions of privacy by industry and government.

The Sony Rootkit controversy, cited elsewhere in this report, generated lots of bad publicity for Sony, the world's second largest record label, which rendered hundreds of thousands of personal computers vulnerable to hacker attack by inserting faulty copy-protection software into its CDs. The bad publicity given to its secret use of copy-

[248] European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006], p. 9 (section 3.3.1). http://ec.europa.eu/information_society/doc/com2006251.pdf

protection technologies, also known as technological protection measures (TPMs), resulted in dozens of class action lawsuits in the United States.

As part of the settlement imposed by the courts, Sony agreed to limitations on its use of TPMs, including improved disclosure requirements, security precautions and privacy safeguards. Purchasers are to be informed on CDs' outer packaging when they contain copy-protection software, which must be pre-approved by an independent oversight party. Users must be informed in plain language of the nature and function of the copy-protection software and of any updates or changes to the copy-protection software. The privacy safeguards were noteworthy since they went beyond the obligations typically found in privacy legislation.[249]

Media interest also played a major role in helping to sink the Bush administration's Total Information Awareness system, developed by the Pentagon for tracking terror suspects, and the Department of Homeland Security's CAPPS II program for screening airline passengers Both programs generated strong objections from civil liberties groups, Congress and the public. Both programs were ultimately scrapped after public outcries over possible threats to privacy and civil liberties.[250]

Public interest in RFIDs and their possible impacts on the privacy of consumers greatly increased as a result of the media interest in a report by an ad hoc group of privacy rights and civil liberties groups in the US, UK, Canada and elsewhere who joined forces as Customers Against Supermarket Privacy Invasion & Numbering (CASPIAN). As a result of media interest and public concerns, RFID suppliers and corporate retailers have been forced to address privacy concerns. Such concerns were inflamed by comments such as this one from Katherine Albrecht, the founder of CASPIAN: "This [RFID] technology is like an electronic frisk or a form of X-ray vision. It really could create a total surveillance world. It's very dangerous."[251] She has dubbed RFIDs as spychips. In the first chapter of her book of the same name, she says "If the master planners have their way, every object—from shoes to cars—will carry one of these tiny computer chips that can be used to spy on you without your knowledge or consent. We've nicknamed these tiny devices 'spychips' because of their surveillance potential."[252]

As RFIDs are a key technology in ambient intelligence, manufacturers, suppliers and network operators must do their utmost not only to counter bad publicity, but also to avoid it. This will best be done by involving privacy advocates and public interest groups at an early stage in the development of new technologies, especially in actively seeking their views about possible impacts and how such impacts are best addressed. Engineers and others should not regard technology as "neutral". New technologies often raise policy issues, and this is certainly true of ambient intelligence. AmI offers great benefits, but the risk of not adequately addressing public concerns could mean delays in implementing the

[249] Geist, Michael, "Sony's mea culpa: Copy-protection settlement lays groundwork for new laws", *The Ottawa Citizen*, 5 Jan 2006.
[250] Lichtblau, Eric and James Risen, "Spy Agency Mined Vast Data Trove, Officials Report", *The New York Times*, 24 Dec 2005. There has been much speculation that, even though the specific programs were killed, the main elements have been subsumed within other programs.
[251] Murray, Charles J., "Privacy Concerns Mount Over Retail Use of RFID", *EE Times*, 1 Dec 2003. http://www.techweb.com/wire/26803432
[252] Albrecht, Katherine and Liz McIntyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, Nelson Current publishers, Nashville, TN, 2005.

technologies, a lack of public support for taxpayer-funded research and vociferous protests by privacy protection advocates.

4.3.16 Cultural safeguards

Cultural artefacts, such as films and novels, may serve as safeguards against the threats and vulnerabilities posed by advanced technologies, including ambient intelligence. Science fiction in particular often presents a dystopian view of the future where technology is used to manipulate or control people, thus, in so doing, such artefacts raise our awareness and serve as warnings against the abuse of technology. A *New York Times* film critic put it this way: "It has long been axiomatic that speculative science-fiction visions of the future must reflect the anxieties of the present: fears of technology gone awry, of repressive political authority and of the erosion of individuality and human freedom."[253]

An example of a cultural artefact is Stephen Spielberg's 2002 film, *Minority Report*, which depicts a future embedded with ambient intelligence, which serves to convey messages or warnings from the director to his audience. *Minority Report* serves up a dystopian, sci-fi view of the future. Some of the technologies seem entirely plausible and, indeed, some of them already exist. One can draw one obvious conclusion from this film, and others like it, i.e., don't trust (rely upon) technology. If it's human, it's fallible. For those sensitive to dark scenarios, *Minority Report* presents an ineluctable but somewhat ambiguous future where the progressive deployment of advanced technologies will further encroach upon our privacy and civil liberties. *Minority Report* is by no means unique as a cultural artefact warning about how future technologies are like a double-edged knife that cuts both ways.

4.4 LEGAL AND REGULATORY SAFEGUARDS

4.4.1 Introduction

At present, the European Union is creating the basic legal framework for the information society. The information society has two important aspects. On the one hand, people increasingly have access to on-line information, products and services (through mobile phones, the Internet, satellites, interactive television…) and on the other, the providers of information society services and governments increasingly have access to information on the citizen (through telecommunication data, location data, cookies…). In the future, the combination of these two information streams may lead to an umbrella network of wirelessly connected objects and subjects that can support all of us in an intelligent, automated and non-obtrusive way.

The fast emergence of information and communication technologies and the growth of on-line communication, e-commerce and electronic services go beyond the territorial borders of the Member States and have led the European Union to adopt numerous legal instruments such as directives, regulations and conventions on e-commerce, consumer protection, electronic signature, cyber crime, liability, data protection, privacy and electronic communication… and many others. Even the European Charter of Fundamental

[253] Scott, A. O., "A Future More Nasty, Because It's So Near", Film review of "Code 46", *The New York Times*, 6 Aug 2004.

Rights will play an important role in relation with the networked information society in the EU.

The existing legal framework has already been extensively discussed in Deliverable 1 of the SWAMI project and its usefulness and effectiveness have been examined in a legal analysis of the dark scenarios in Deliverable 2 of the SWAMI Project.[254] These exercises have pointed out that there *are* threats and vulnerabilities in ambient intelligence and that we may encounter serious legal problems when applying the existing legal framework. While AmI requires the automatic processing of as much of the available data as possible, the obligations imposed by current legislation on processing of data could impose too big burden for undertakings and consumers, and quickly lead to an information overflow. Another serious problem is that the European legal framework applies only to a limited number of countries.

These threats and vulnerabilities derive from the fact that we are, on the one hand, confronted with new technologies and, on the other, with the presumption that certain human values such as privacy, security and identity remain existent, in some form or other. These legal safeguards are largely based on this presumption.[255]

We will draw attention to the conclusions previously derived from these exercises and we will propose possible *approaches* to solutions for some previously identified threats and vulnerabilities. We describe these approaches as *safeguards*.

The proposed safeguards should be considered as general policy options, aimed at stimulating discussion between stakeholders and, especially, policy-makers. Though our proposals do not cover all relevant safeguards, they contain the safeguards that are in any event instrumental for an adequate legal framework. Moreover, we don't aspire to achieve the kind of precision that is needed for drafting legislative texts, for which further in-depth analysis is necessary. In addition, most of the *legal* safeguards we propose need the support of technology as well as of social (education) and economic safeguards in order to take effect.

4.4.2 General recommendations

Law and architecture go together (Recommendation 1)

Regulating ambient intelligence is far from being an exclusive legal exercise. On the contrary: law is only one of the available sets of tools for regulating behaviour, next to social norms, market rules, "code"[256] – the architecture of the technology (e.g., of cyberspace, wireless and wired networks, security design, encryption levels, rights

[254] http://swami.jrc.es.

[255] "Assessing IT is therefore by the very nature of the subject a tightrope walk between identifying a process marked by radical changes (e.g. papyrus, printing press, telegraph, television, Internet, ...) on the one hand, and a view focusing on the invariants of human behaviour." Kündig, A., *A Basis for IT Assessment. An overview of the underlying technologies, their applications and the implications for individuals, society and business*, Swiss Centre for Technology Assessment, 2002, 3 (46 p.), http://www.ta-swiss.ch/www-remain/reports_archive/publications/2002/TA43_2002.pdf.

[256] Lessig, Lawrence, "The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 133, 1999, pp. 501-546. See also Brownsword, Roger, "Code, control, and choice. Why East is East and West is West", *Legal Studies*, Vol. 25 No 1, March 2005, pp. 1-21.

management systems, mobile telephony systems, user interfaces, biometric features, handheld devices, accessibility criteria, etc) and many other tools.

The regulator of ambient intelligence can, for instance, achieve certain aims directly by imposing laws, but also indirectly by, for example, influencing the rules of the market. Regulatory effect can also be achieved by influencing the architecture of a certain environment. The relationship between law and architecture merits our attention. On the one hand, the architecture of AmI might well make certain legal rules difficult to enforce (for example, the enforcement of data protection obligations on the Internet or the enforcement of copyright in peer-to-peer networks), and might cause new problems, particularly related to the new environment (spam, dataveillance). On the other hand, the "code" has the potential to regulate by enabling or disabling certain behaviour, while law regulates via the threat of sanction. In other words, software and hardware constituting the "code", and architecture of the digital world, causing particular problems, can be at the same time the instrument to solve them. Regulating through code may have some specific advantages: Law traditionally regulates ex post, by imposing a sanction on those who did not comply with its rules (in the form of civil damages or criminal prosecution). Architecture regulates by putting conditions on one's behaviour, allowing or disallowing doing something, not allowing the possibility to disobey. It regulates ex ante.

Ambient intelligence is particularly built on software code. This code influences how ambient intelligence works, e.g., how the data are processed, but this code itself can be influenced and accompanied by regulation.[257] Thus, the architecture can be a tool of law. This finding is more than elementary. It shows that there is a choice: should the law change because of the "code"? Or should the law change "code" and thus ensure that certain values are protected? Should the socio-economic environment and condition be changed? Today, it seems that we are often confronted with the first approach: the growing data processing infrastructure seems to erode privacy and data protection law to such an extent that policy-makers are inclined to change data protection law (e.g., by imposing data retention on communication providers since traffic and location data are available). However, one could also give example of the law affecting "code". This already happens, e.g., in the field of telecommunications by requiring phone operators to make wire-tapping possible or by imposing e.g. on phone operators that, "where presentation of calling line identification is offered, the service provider must offer the calling user the possibility … of preventing the presentation of the calling line identification on a per-call basis"[258].

The development of technology represents an enormous challenge for privacy, enabling increasing surveillance and invisible collection of data. A technology that threatens privacy may be balanced by the use of a privacy enhancing technology: the "code", as Lessig claims, can be the privacy saviour. Leenes and Koops have undertaken a critical analysis of this optimistic view on "code" as a privacy safeguard.[259] These authors point out that the relation between code and privacy is not as straightforward as in other domains, for

[257] Contrary to the long-lasting paradigm, as the Lessig writes. Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999, and "Commentaries, The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 113:501, 1999, pp. 501-546

[258] Telecom operators and device manufacturers must thus provide software and architecture that allow users to switch the caller line identififcation off. See Article 8 of Directive 2002/58 of 12 July 2002 on Privacy and Electronic Communications.

[259] Leenes, R., and B.J. Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, pp. 239-340.

example, in intellectual property law and digital rights management systems (DRMs). There are examples of privacy-protecting technologies. Leenes and Koops discuss privacy codes such as the Platform for Privacy Preferences Project (P3P) that "enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents".[260] Other technologies aim to limit the amount of data actually collected to the necessary minimum (biometric template stored on the card rather than in the central database; browser programs that allow blocking of cookies). However, most of the current technologies simply ignore the privacy implications and collect personal data when there is no such need. There is also a wrong paradigm: the conviction that the user identity is needed to provide the service in all situations, e.g., in the case of access to (freely available) information. A shift of the paradigm to privacy-by-design is necessary to effectively protect privacy. Indeed, technology can facilitate privacy friendly verification of individuals via, e.g., anonymous and pseudonymous credentials. Leenes and Koops recognise the potential of these privacy-enhancing technologies (PETs) to enforce data protection law and privacy rules. But they also point at problems regarding the use of such technologies, which are often troublesome in installation and use for most consumers. Moreover, industry is not really interested in implementing privacy-enhancing technology. They see no (economic) reason to do it.

The analysis of Leenes and Koops shows that neither useful technology, nor law is sufficient in itself. Equally important is raising stakeholder awareness, social norms and market rules. All regulatory means should be used and have to be used to respond to problems of the new environment to tackle it effectively. The SWAMI consortium agrees with such an approach, and tries to promote all available tools of regulation to respond to the needs of AmI. *For the full effectiveness of any regulation, one should always look for the optimal mixture of all accessible means.*[261] We are also optimistic and believe there is need *and* possibility to preserve values of privacy. "Code" and PETs might bring valuable input to achieve the aims of privacy and data protection laws. However, influencing the architecture is not enough. An adequate legal framework, independent from the code, is still needed.

Precaution or caution through opacity? (Recommendation 2)

The application of the precautionary principle (originally established as a legal principle for environmental problems) to ICT problems and AmI can certainly be considered. As the impact and effects of the large-scale introduction of AmI in societies spawn a lot of uncertainties, the careful demarche implied of the precautionary principle, with its information, consultation and participation constraints, might be appropriate. However, the application of this principle outside the scope of environmental law is still under debate. Yet, it might inspire us in devising legal policy options when, as regards AmI, fundamental choices between opacity tools and transparency tools must be made.[262] Opacity tools proscribe the interference by powerful actors into the individual's autonomy, while transparency tools accept such interfering practices, though under certain conditions which guarantee the control, transparency and accountability of the interfering activity and actors.

---

[260] www.w3.org/P3P

[261] Lessig, L.,"Commentaries, The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 113:501, 1999, pp. 501-546

[262] De Hert, Paul, & Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in Erik Claes, Anthony Duff & Serge Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, pp. 61-104.

Europe, like all constitutional systems, uses both tools at the same time. The articulation of the right to privacy (an opacity tool) and data protection law (a transparency tool) should be understood along those lines.

In our opinion, most of the challenges arising in the new AmI environment should be addressed by transparency tools (such as data protection and security measures). Transparency should be the default position, although some prohibitions referring to political balances, ethical reasons or core legal concepts should be considered too.

Legal scholars don't discuss law in general terms. Their way of thinking always involves an application of the law in concrete or exemplified situations. In fact, applying actual law to actual situations (which is the work of judges in real case scenarios) is not that different from applying actual law to future situations (which is done in this project by drafting future scenarios and comparing these scenarios with actual law). This means that there will not be something like an "advocacy against ambient intelligence". The legislator will compare concrete examples and situations with the law and will not try to formulate general positions or policies. For instance, instead of determining whether or not a foetus constitutes human life, legislators and judges will determine at which stage of the pregnancy abortion is allowed, and at which stage abortion is not acceptable. Thus, the proposed legal framework will not deal with the AmI problems in a general way, but focus on concrete issues, and apply opacity and transparency solutions accordingly.

Central lawmaking for AmI is not recommended (Recommendation 3)

Another particularity of legal regulation in cyberspace is the absence of a central legislator. In Europe, the legislative powers are exercised by the Member States, though some powers have been transferred to the European Union. On the other hand, international drivers such as technology producers and firms or institutions such as the G7 have a more than considerable impact on the new environment. Though our legal analysis is based mostly on European law, we emphasise that not everything is regulated at a European level. Regulation of (electronic) identity cards, for instance, concerns a crucial element in the construction of an AmI environment, but is within the powers of the individual Member States.

Both at European and national level, some decision-making competences have been delegated to independent advisory organs (children's rights commissioners, data protection authorities). Hence, there exist many, what we can call, 'little legislators' that adjust in some way the often executive power-origin of legislation: The Article 29 Data Protection Working Party, national children's rights commissioners and international standardisation bodies can and do, for example, draft codes of conduct that constitute often (but not always) the basis for new legislation.

The SWAMI consortium does not suggest the centralisation of the law-making process. On the contrary, we recommend respect for the diversity and plurality of lawmakers. The solutions produced by the different actors should be taken into consideration and be actively involved in policy discussions. Development of case law should also be closely observed. Consulting concerned citizens and those who represent citizens (including legislators) at the stage of development would increase the legitimacy of new technologies.

4.4.3 Preserving the core of privacy and other human rights

Recommendations regarding privacy

Privacy aims to ensure no interference in private and individual matters. It offers an instrument to safeguard the opacity of the individual and puts limits to the interference by the powerful actors into the individual's autonomy. Normative in nature, regulatory opacity tools should be distinct from regulatory transparency tools, of which the goal is to control the exercise of power rather than to restrict power.[263]

We observe today that the reasonable expectation of privacy erodes[264] due to emerging new technologies and possibilities for surveillance: it develops into an expectation of being monitored. Should this, however, lead to diminishing the right to privacy? Ambient intelligence may seriously threaten this value, but the need for privacy (e.g., the right to be let alone) will probably remain, may it be in another form adapted to new infrastructures (e.g., the right to be left off-line).

The right to privacy in a networked environment could be enforced by any means of protecting the individual against any form of dataveillance.[265] Such means are in line with the data minimisation principle of data protection law, which is a complementary tool to privacy. However, in ambient intelligence where collecting and processing personal data is almost a prerequisite, new tools of opacity such as the right to be left 'off-line' (in time – e.g., during certain minutes at work – or in space, e.g., in public bathrooms) could be recognised.

Several instruments of opacity can be identified. We list several examples, and there may be other examples. Additional opacity recommendations are made in subsequent sections,

---

[263] "'Opacity' designates a zone of non-interference which in our opinion must not be confused with a zone of invisibility: privacy, for instance, does not imply secrecy; it implies the possibility of being oneself openly without interference. Another word might have been "impermeability" which is too strong and does not contrast so nicely with "transparency" as "opacity" does. See Hildebrandt, M., and S. Gutwirth (eds.), *Implications of profiling on democracy and the rule of law*, FIDIS (Future of Identity in the Information Society), Deliverable D7.4, September 2005. http://www.fidis.net. See also De Hert P. & S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2005, pp. 61-104; De Hert P. & S. Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence" in *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Institute for Prospective Technological Studies - Joint Research Centre, Seville, July 2003, pp. 111-162 (ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf) and Gutwirth, S., "De polyfonie van de democratische rechtsstaat" [The polyphony of the democratic constitutional state] in M. Elchardus (ed.), *Wantrouwen en onbehagen* [Distrust and uneasiness], Balans 14, VUBPress, Brussels, 1998, pp.137-193.

[264] See Punie Y., S. Delaitre, I. Maghiros & D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D 2, November 2005, Scenario 1 situation 2, p. 18 and p. 77.

[265] "Dataveillance means the systematic monitoring of people's actions or communications through the application of information technology", M. Hansen and H. Krasemann (eds.), *Privacy and Identity Management for Europe - PRIME White Paper - Deliverable 15.1.d.,* 18 July 2005, p. 11 (35 p.), with a reference to Clarke, R., "Information Technology and Dataveillance", *Communications of the ACM*, 31(5), May 1988, pp. 498-512, and re-published in C. Dunlop and R. Kling (eds.), *Controversies in Computing*, Academic Press, 1991 available at http://www.anu.edu/people/Roger.Clarke/DV/CACM88.html;

for example, with regard to biometrics. We observe that there is not necessarily an internal coherence between the examples listed below. The list should be understood as a wish list or a list with suggestions to be consulted freely.

Recommendation regarding digital territories

The concept of a digital territory represents a vision that introduces the notions of space and borders in future digitised everyday life. It could be visualised as a bubble, whose boundaries and transparency depends on the will of its owner. The notion of a digital territory aims for a "better clarification of all kinds of interactions in the future information society. Without digital boundaries, the fundamental notion of privacy or the feeling of *being at home* will not take place in the future information society".[266] The concept of digital territories encompasses the notion of a virtual residence, which can be seen as a virtual representation of the smart home.[267]

The concept of digital territories could provide the individual with a possibility to access to – and stay in – a private digital territory of his own at (any) chosen time and place. This private, digital space could be considered as an extension of the private home. Today, already, people indeed store their personal pictures on distant servers; read their private correspondences online; provide content providers with their watching/consuming behaviour for the purpose of digital rights management; communicate with friends and relatives through instant messengers and Internet telephony services. The "prognosis is that the physical home will evolve to 'node' in the network society, implying that it will become intimately interconnected to the virtual world."[268]

The law guarantees neither the establishment nor the protection of an online private space in the same way as the private space in the physical world is protected. Currently, adequate protection is lacking.[269] For example, telecommunication service providers will have to keep communication data at the disposal of law enforcement agencies (data retention law). The retention of communication data relates to mobile and fixed phone data, Internet access, -mail and –telephony. Data to be retained includes the place, time, duration and destination of communications. What are the conditions for accessing such data? Is the individual informed when such data are accessed? Does he have the right to be present when such data are examined? Does the inviolability of the home extend to the data that are stored on a distant server? Another example of the inadequate protection concerns the increasing access to home activities from a distance, e.g., as a result of the communication data generated by domestic applications that are connected to the Internet. In both examples, there is no physical entrance in the private place.[270]

---

[266] Beslay, L., and H. Hakala, "Digital Territory: Bubbles", p. 11, draft version available at http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf.
[267] Idem.
[268] De Hert, P. & S. Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence", *l.c.*, p. 159.
[269] Idem. *See also* Beslay, L. & Y. Punie, "The Virtual Residence: Identity, Privacy and Security", *Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview*, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, p. 67. http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html.
[270] See Koops, B.J. & M.M. Prinsen, "Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit" ["Glass house, transparent body. A future view on home law and body integrity"], *Nederland Juristenblad*, 12 March 2005, pp. 624-630.

To ensure that these virtual private territories become effectively a private domain for the individual, a regulatory framework could be established to prevent unwanted and unnoticed interventions similar to the one that currently applies to the inviolability of the private home.

A set of rules needs to be envisaged to guarantee such protection, amongst them, the procedural safeguards similar to those currently applicable to the protection of our homes against state intervention (e.g., requiring a search warrant). Technical solutions aimed at defending private digital territories against intrusion should be encouraged and, if possible, legally enforced.[271] *The individual should be empowered with the means to freely decide what kind of information he or she is willing to disclose, and that aspect should be included in the digital territory concept. Similarly, vulnerable home networks should be granted privacy protection. Such protection could also be extended to the digital movements of the person, that is, just as the privacy protection afforded the home has been or can be extended to the individual's car, so the protection could also be extended to home networks, which might contact external networks.*[272]

Recommendation regarding spy-free territories for workers and children

Privacy at the workplace has already been extensively discussed.[273] Most of the legal challenges that may arise can be answered with legal transparency rules, as discussed above. However, certain more drastic, prohibitive measures may be necessary in certain situations involving too far-reaching or unnecessary surveillance, which a society considers as infringing upon the dignity of the employee. *One of the ways to grant the individual a possibility to escape such disproportional surveillance at the workplace is obliging organisations to create physical spaces at work without surveillance technology, e.g., in social areas where the individual can relax and take a short break and in the bathrooms. The idea of cyber territories, accessible to the individual when he is in the workplace, would grant him the possibility of being alone in his private digital or cyber activities.*[274]

In addition, transparency rules are needed to regulate other, less intrusive problems. We recall here the specific role of law-making institutions in the area of labour law. Companies must discuss their surveillance system and its usage in collective negotiations with labour organisations and organisations representing employers before its implementation in a company or a sector, taking into account the specific needs and risks

[271] De Hert, P. & S. Gutwirth, "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence", in *Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview*, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, p. 159.
ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf

[272] Beslay, L., & Y. Punie, "The Virtual Residence: Identity, Privacy and Security", IPTS Report 67. http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html

[273] Punie Y., S. Delaitre, I. Maghiros, & D. Wright, (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D 2, November 2005, paragraph 6.1.1, p. 78. See also Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace* (5401/01/EN/Final - WP 55), adopted 29 May 2002, available through http://ec.europa.eu/justice_home/fsj/privacy/.

[274] A similar recommendation has been proposed by the Article 29 Data Protection Working Party in *Working Document on the Processing of Personal Data by means of Video Surveillance* (11750/02/EN - WP 67), adopted 25 November 2002, available through http://ec.europa.eu/justice_home/fsj/privacy/.

involved (e.g., workers in a bank vs. workers in public administration). *All employees should always be clearly and a priori informed about the employee surveillance policy of the employer in that respect (when and where surveillance is taking place, what is the finality, what information is collected, how long it will be stored, what are the (procedural) rights of the employees when personal data are to be used as evidence, etc.).*[275]

Specific cyber territories for children have to be devised along the same lines. The United Nations Convention on the Rights of the Child (1990) contains a specific privacy right for children, and sets up monitoring instruments such as National Children's Rights Commissioners. Opinions of such advisory bodies should be carefully taken into account in policy discussion. National Children's Rights Commissioners could take up problems relating to the permanent digital monitoring of children.

Recommendation regarding restrictions on use of illegally obtained evidence

As pointed out in the first deliverable of the SWAMI project, courts are willing to protect one's privacy but, at the same time, they tend to admit evidence obtained through a violation of privacy or data protection.[276] There is a lack of clarity and uniformity regarding the consequence of privacy violations.

The European Court of Human Rights is unwilling to recognise a right to have evidence obtained through privacy violations rejected.[277] This line of reasoning is followed by at least some national courts.[278] The fact that there is no general acceptance of an exclusionary rule creates legal uncertainty. Its general acceptance is, however, necessary to protect the opacity of the individual in a more effective way.

The departure from such position by the courts (namely 'no inclusion of evidence obtained through privacy and/or data protection law infringements') could be considered and legislative prohibition of the admissibility (or general acceptance of the exclusionary rule) of such obtained evidence envisaged.[279]

---

[275] Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace* (5401/01/EN/Final - WP 55), adopted 29 May 2002, available through http://ec.europa.eu/justice_home/fsj/privacy/.

[276] Punie Y., S. Delaitre, I. Maghiros & D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D 2, November 2005, paragraph 6.1.1, p. 78.

[277] In fact in the case of *Khan* v. *United Kingdom,* judgement of 12 May 2000, the court rejected the exclusionary rule. In that case, the evidence was secured by the police in a manner incompatible with the requirements of Article 8 of the Convention. The court accepted that the admission of evidence obtained in breach of the privacy right is not necessarily a breach of the required fairness under Article 6 of ECHR (the right to a fair trial), since the process taken as a whole was fair in the sense of Article 6. The evidence against the accused was admitted and led to his conviction. The Khan doctrine (followed in cases such as Doerga v. the Netherlands and P.G. and J.H. v. The United Kingdom) is discussed in De Hert, P., "De soevereiniteit van de mensenrechten: aantasting door de uitlevering en het bewijsrecht" [Sovereignty of human rights: threats created by the law of extradition and by the law of evidence], Panopticon, *Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, Vol. 25, No. 3, 2004, pp. 229-238 and in De Hert P. & F.P. Ölcer, "Het onschadelijk gemaakte Europees privacybegrip. Implicaties voor de Nederlandse strafrechtspleging" [The notion of privacy made innocent. Implications for criminal procedure], *Strafblad. Het nieuwe tijdschrift voor strafrecht,* Vol. 2, No 2, 2004, pp. 115-134. See also De Hert, P., *Biometrics: legal issues and implications,* Background paper for the Institute of Prospective Technological Studies, DG JRC, European Commission, Sevilla, January 2005, p. 33.

[278] Cour de Cassation (Belgium) 2 March 2005, http://www.juridat.be.

[279] Although such a finding seems to contradict current case law (such as the Khan judgement, refusing to apply the principle that illegally obtained privacy evidence should be rejected).

Recommendations regarding implants

In ambient intelligence, the use of implants can no longer be considered as a kind of futuristic or extraordinary exception. Whereas it is clear that people may not be forced to use such implants, people may easily become willing to equip themselves with such implants on a (quasi) voluntary basis, be it, for example, to enhance their bodily functions or to obtain a feeling of security through always-on connections to anticipate possible emergency situations. Such a trend requires a careful assessment of the opacity and transparency principles (as explained above) at a national, European and international level.

Currently, in Europe, the issue of medical implants has already been addressed.[280] In AmI, however, implants might be used for non-medical purposes. One of the SWAMI scenarios shows that organisations could be willing to force people to have an implanted device, for example, to be localised anywhere and any time. An employer could require this from his employees, an insurance company from its customers, imposing this as a requirement to obtain better contractual conditions. This could create the possibility of monitoring people (and possibly their physical condition) at any time and in any place... However, in any case, precision and carefulness are well advised.

Now, the law provides for strict safety rules for medical implants. The highest standards of safety should be observed in AmI. The European Group on Ethics in Science and New Technologies also recommends applying the precautionary principle as a legal and ethical principle when it considers the use of implantable technologies. It also reminds us that the principles such as data minimisation, purpose specification, proportionality and relevance are in particular applicable to implants. It means, inter alia, that implants should only be used when the aim cannot be achieved by less body-intrusive means. Informed consent is necessary to legitimise the use of implants. We agree with those findings.

The European Group on Ethics in Science and New Technologies goes further, stating that non-medical (profit-related) applications of implants constitute a potential threat for human dignity and even for a democratic society. Applications of implantable surveillance technologies are only permitted when there is an urgent and justified necessity in a democratic society, and must be specified in legislation.[281] Building on those comments, we agree that the above-mentioned applications should be diligently scrutinised.

We propose that the appropriate authorities (e.g., the Data Protection Officer) control and authorise applications of implants after the assessment of the particular circumstances in each case. When an implant enables tracking of people, people should have the possibility to disconnect the implant at any given moment and they should have the possibility to be informed when a (distant) communication (e.g., through RFID) is taking place.

[280] Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active medical devices, *Official Journal* L 323 , 26 November 1997, p. 39

[281] European Group on Ethics in Science and New Technologies, "Ethical Aspects of ICT Implants in the Human Body", Opinion to the Commission, 16 March 2005.
http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf

We agree with the European Group on Ethics in Science and New Technologies that irreversible ICT implants should not be used, except for medical purposes. Further research on the long-term impact of ICT implants is also recommended.[282]

Recommendations regarding anonymity, pseudonymity, credentials and trusted third parties

Another safeguard to guarantee the opacity of the individual is the possibility to act under anonymity (or at least under pseudonymity or 'revocable anonymity'). Anonymity is crucial for ambient intelligence; its importance has already been tackled in previous chapters.

The Article 29 Working Party, in one of its first recommendations after its establishment on the basis of Article 29 of the 1996 data protection directive, already considered anonymity as an important safeguard for the right to privacy. We can repeat here its recommendations:
(a) The ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on-line as they currently enjoy off-line.
(b) Anonymity is not appropriate in all circumstances.
(c) Legal restrictions which may be imposed by governments on the right to remain anonymous, or on the technical means of doing so (e.g., availability of encryption products) should always be proportionate and limited to what is necessary to protect a specific public interest in a democratic society.
(d) The sending of e-mail, the passive browsing of world-wide web sites, and the purchase of most goods and services over the Internet should all be possible anonymously.
(e) Some controls over individuals contributing content to on-line public fora are needed, but a requirement for individuals to identify themselves is in many cases disproportionate and impractical. Other solutions are to be preferred.
(f) Anonymous means to access the Internet (e.g., public Internet kiosks, pre-paid access cards) and anonymous means of payment are two essential elements for true on-line anonymity.[283]

According to the Common Criteria for Information Technology Security Evaluation Document (ISO 15408),[284] anonymity is only one of the requirements for the protection of privacy, next to pseudonymity, unlinkability, unobservability, user control/information management and security protection. All these criteria should be considered as safeguards for privacy.[285]

The e-signature directive promotes the use of pseudonyms and, at the same time, aims to provide security for transactions. *The probative value of digital signatures is regulated differently under the national laws of Member States.*[286] *More clarity as to the legal value of electronic signatures would be desirable, so that its admissibility as evidence in legal*

[282] Idem.
[283] Article 29 Data Protection Working Party, *Recommendation 3/97: Anonymity on the Internet* (WP 6), adopted on 3 December 1997, available through http://ec.europa.eu/justice_home/fsj/privacy/.
[284] ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*, First edition, International Organization for Standardization, Geneva, 1999.
[285] See also under 4.3.3.
[286] The German example was described in: Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, p. 29. http://www.fidis.net

proceedings is fully recognised.[287] *The status of pseudonymity under the law needs further clarification. A pseudonym prevents disclosure of the real identity of a user, while still enabling him to be held responsible to the other party if necessary. It may provide a privacy tool, and remedy against profiling. Using different pseudonyms also prevents the merging of profiles from different domains. It is, however, unclear what is the legal status of pseudonyms (whether they should be regarded as anonymous data or as personal data falling under the data protection regime). Clarification of the issue is desirable.*[288]

In ambient intelligence, the concept of *unlinkability* can become as important as the concept of anonymity or pseudonymity. Moreover, anonymity and pseudonymity may perhaps only protect individuals if this anonymity or pseudonymity is accompanied by the unlinkability of the anonymous or pseudonymous data. Unlinkability "ensures that a user may make multiple uses of resources or services without others being able to link these uses together.... Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system."[289] When people act pseudonymously or anonymously, their behaviour in different times and places in the ambient intelligence network could still be linked and consequently be subject to control, profiling and automated decision-making: linking data relating to the same *non-identifiable* person may result in similar privacy threats as linking data that relate to an identified or identifiable person.

Thus, in addition to and in line with the right to remain anonymous goes the use of anonymous and pseudonymous credentials, accompanied with unlinkability in certain situations (e.g., e-commerce), reconciling thus the privacy requirements with the accountability requirements of, e.g., e-commerce. In fact, such mechanisms should always be foreseen when disclosing someone's identity or when linking the information is not necessary. Such necessity should not be easily assumed, and in every circumstance more privacy-friendly technological solutions should be sought.[290] *However, the use of anonymity should be well balanced. To avoid its misuse, digital anonymity could be further legally regulated, especially stating when it is not appropriate.*[291]

---

[287] Currently the directive on electronic signatures states that only advanced electronic signatures (those based on a qualified certificate and created by a secure signature-creation device) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data and are admissible as evidence in legal proceedings. Member States must ensure that an electronic signature (advanced or not) is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: (a) in electronic form, (b) not based upon a qualified certificate, (c) not based upon a qualified certificate issued by an accredited certification service-provider, or (d) not created by a secure signature creation device.

[288] Olsen T., T. Mahler, et al, "Privacy – Identity Management, Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", LEGAL IST: LEGAL Issues for the Advancement of Information Society Technologies, Deliverable D11, 2005. See LEGAL IST website http://193.72.209.176/default.asp?P=369&obj=P1076

[289] ISO99 ISO IS 15408, 1999. http://www.commoncriteria.org/. See also Pfizmann, A. and M. Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology,* Version v0.27, 20 Feb. 2006. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. Pfizmann and Hansen define unlinkability as follows: "*Unlinkability* of two or more items (e.g., subjects, messages, events, actions, ...) means that within the system (comprising these and possibly other items), from the attacker's perspective, these items are no more and no less related than they are related concerning his a-priori knowledge."

[290] Leenes, Ronald And Bert-Jan. Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, p.37.

[291] Compare Gasson, M., M. Meints and K. Warwick, (eds.), "A study on PKI and biometrics", FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, pp. 35-36. http://www.fidis.net

Recommendation regarding criminal liability rules

Provisions on criminal liability are necessary to prevent cybercrime. The criminal law is a basic means to fight hackers, attackers and others tending to abuse the possibilities of communication. Moreover, *effective* criminal provisions have a general deterrent effect, thus stopping people from undertaking criminal activities.

Cybercrime has cross-border dimensions and global implications. The restrictive interpretation of criminal laws ('nulla poena sine crimen') requires international consensus on the definition of the different crimes. This issue has been addressed extensively by the Cybercrime Convention[292], which provides a definition for several criminal offences related to cybercrime and for general principles concerning international co-operation. The Cybercrime Convention, however, allows for different standards of protection. The Convention obliges its signatories to criminalise certain offences under national law, but member states are, however, free to narrow the scope of the definitions by introducing some additional requirements. The most important weakness of this Convention is the slow progress in its ratification by signatory states. This makes this international instrument rather ineffective.

Council Framework Decision 2005/222/JHA also provides for criminal sanctions against cybercrimes. 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 highly recommended that governments ensure a proper ratification of the Convention. A "revision" mechanism would desirable so that signatories could negotiate and include in the convention definitions of new, emerging cybercrimes. Specific provisions criminalising identity theft and (some forms of) unsolicited communication could be included within the scope of the convention.

International co-operation in preventing, combating and prosecuting criminals is needed and may be facilitated by a wide range of technological means, but these new technological possibilities should not erode the privacy of innocent citizens who are deemed to be not guilty until proven. Cybercrime prosecution, and more importantly crime prevention might be facilitated by a wide range of technological means, among them, those that provide for the security of computer systems and data against attacks.[293]

4.4.4 Specific recommendations regarding data protection

Introduction

One can say that almost all human activities in ambient intelligence can be reduced to personal data processing: opening doors, sleeping, walking, eating, putting lights on, shopping, walking in a street, driving a car, purchasing, watching television and even breathing. In short, all physical actions become digital information that relates to an identified or identifiable individual.

[292] Council of Europe - Cybercrime Convention of 23 November 2001.
[293] Pfitzmann, A. and M. Kohntopp, "Striking a Balance between Cyber-Crime and Privacy", *IPTS Report* 57, EC-JRC, Seville, Sept 2001. http://www.jrc.es/home/report/english/articles/vol57/welcome.htm

Often, the ambient intelligence environment will need to adapt to individuals and will therefore use profiles applicable to particular individuals (personal profiles) or to all individuals that fall within a group profile.[294] AmI will change not only the amount, but also the quality of data collected so that we can be increasingly supported in our daily life (the goal of ambient intelligence). AmI will collect (and need to collect) data not only about what we are doing, when we do it and where we are, but also data on how we have experienced things.[295] One can assume that the accuracy of the profiles, on which the personalisation of services depends, will improve as the amount of data collected grows. But as others hold more of our data, so grows the privacy risks. Thus arises the fundamental question: Do we want to minimise personal data collection?

Instead of focusing on reducing the amount of data collected, should we admit that they are indispensable for the operation of AmI, and focus rather on preventing undesirable processing of such data by empowering the user with a means to control such processing of personal data?

Data protection is a tool for empowering the individual in relation to the collection and processing of his or her personal data. The European data protection directive imposes a set of obligations on the data controller and supports the rights of the data subject with regard to the transparency and control over the collection and processing of data. It does not provide for prohibitive rules on data processing (except for the processing of sensitive data and the transfer of personal data to third countries that don't ensure an adequate level of protection). Instead, the EU data protection law focuses on a regulatory approach and on channelling, controlling and organising the processing of personal data. As the title of Directive 95/46 indicates, the directive concerns both the protection of the individual with regard to the processing of personal data *and* the free movement of such data. The combination of these two goals in Directive 95/46 reflects the difficulties we encounter in the relations between ambient intelligence and data protection law.

There is no doubt that some checks and balances in using data should be put in place in the overall architecture of the AmI environment. Civil movements and organisations dealing with human rights, privacy or consumer rights, observing and reacting to the acts of states and undertakings might provide such guarantees. It is also important to provide incentives for all actors to adhere to the legal rules. Education, media attention, development of good practices and codes of conducts are of crucial importance to achieve this aim. Liability rules (discussed in detail below), and rules specifically aimed at enforcement of the data protection obligations (e.g., in regard to data laundering) will become very important.

Data protection law provides for the right to information, access or rectification, which constitute important guarantees of individual rights. However, its practical application in an AmI era could easily lead to an administrative nightmare, as information overload

---

[294] See Hildebrandt, M. and J. Backhouse (eds.), *Descriptive analysis and inventory of profiling practices*, FIDIS (Future of Identity in the Information Society) Deliverable D7.2; Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS Deliverable D7.3. Chapter 7 of this deliverable deals with legal issues on profiling. See also Hildebrandt, M. and S. Gutwirth (eds.), *Implications of profiling on democracy and the rule of law*, FIDIS Deliverable D7.4, September 2005. http://www.fidis.net.

[295] Lahlou, Saadi, Marc Langheinrich and Carsten Rocker, "Privacy and Trust Issues with Invisible Computers", *Communications of the ACM*, Vol. 48 No. 3, March 2005, pp. 59-60.

would make it unworkable. Since we recognise the right to information as one of the basic guarantees of individual rights, we should try to remedy such a situation in a way that does not diminish this right.

The right to be informed

The right to be informed is one of the principles of the European data protection law. The individual's right to information is a prerequisite to protect his interests. Such a right corresponds to a decentralised system of identity (data) management, but it seems useful to tackle it separately to emphasise the importance of the individual's having access to information about the processing of his data. Because of the large amounts of data to be processed in an AmI world, the help of or support by intelligent agents to manage such information streams seems indispensable.

The obligation to inform the data subject about when and which data are collected, by whom and for what purpose gives the data subject the possibility to react to mistakes (and thus to exercise his right to rectification of data) or abuses, and enables him to enforce his right in case of damage. It would actually be desirable to provide the individual not only with information about what data relating to him are processed, but also what knowledge has been derived from the data.

Information about what knowledge has been derived from the data could help the individual in proving causality in case of damage. Further research on how to reconcile access to the knowledge in profiles (which might be construed as a trade secret in some circumstances) with intellectual property rights would be desirable.

Information notices

The right to be informed could be facilitated by providing information in a machine-readable language, enabling the data subject to manage the information flow through or with the help of (semi-) autonomous intelligent agents. Of course, this will be more difficult in situations of passive authentication, where no active involvement of the user takes place (e.g., through biometrics and RFIDs).

Thus, information on the identity of the data controller and the purposes of processing could exist both in a human-readable and in a machine-readable language. Although we consider the broad range of information as useful for the data subject and software assistance necessary in the long run, we also recognise the way such information is presented to the user is of crucial importance.

In that respect, the Article 29 Working Party has provided useful guidelines and proposed multi-layer EU information notices.[296] Such notices would essentially consist of three layers:

[296] Article 29 Data Protection Working Party, *Opinion on More Harmonised Information Provisions* (11987/04/EN - WP 100), adopted on 25 November 2004, available through http://ec.europa.eu/justice_home/fsj/privacy/; Article 29 WP also proposes the examples of such notices (appendixes to the opinion on More Harmonised Information Provisions). See also Meints, M., "AmI – The European Perspective on Data Protection Legislation and Privacy Policies", presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006, available at http://swami.jrc.es/pages/deliverables.htm (Report of the final conference).

Layer 1 – The short notice contains core information required under Article 10 of the Data Protection Directive (identity of the controller, purpose of processing, or any additional information which, in the view of the particular circumstances of the case, must be provided to ensure fair processing). A clear indication must be given as to how the individual can access additional information.

Layer 2 – The condensed notice contains all relevant information required under the Data Protection Directive. This includes the name of the company; the purpose of the data processing; the recipients or categories of recipients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the possibility of transfer to third parties, the right to access, to rectify and oppose; choices available to the individual. In addition, a point of contact must be given for questions and information on redress mechanisms either within the company itself or details of the nearest data protection agency.

Layer 3 – The full notice includes all national legal requirements and specificities. It could contain a full privacy statement with possible additional links to national contact information.

We recommend that industry and law enforcement agencies consider this idea, based on the P3P platform, for AmI environments. Electronic versions of such notices should be sufficient in most of circumstances.

Data laundering obligations

The scenarios, described in SWAMI Deliverable 2, highlighted a new kind of practice that has emerged during the last years, in the sector of personal data trading: while some companies collect personal data in an illegal way (not informing the data subjects, transferring to third parties without prior consent, usage for different purposes, installing spyware, etc.), these personal data are shared, sold and otherwise transferred throughout a chain of existing and disappearing companies to the extent that the origin of the data and the original data collector cannot be traced back. This practice has been described as "data laundering", with analogy to money laundering: it refers to a set of activities aiming to cover the illegitimate origin of data. In ambient intelligence, the value of personal data and therefore the (illegal) trading in these data will (probably) only but increase.

A means to prevent data laundering could be creating 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 and thus held liable for illegal data processing. An obligation could be created to notify the national Data Protection Officers when personal data(bases) are acquired. We could foresee that the persons and companies involved or assisting in data laundering are subject to criminal sanctions.

Restricted interoperability

SWAMI recognises that AmI requires efficient, faultless and quick exchanges of relevant data and information throughout the AmI network. The need for efficiency requires interoperable data formats and interoperable hardware and software for data processing. The first SWAMI scenario about the bus accident has shown the need for interoperability in ambient intelligence. But fully operational generalised interoperable ambient intelligence, in which data and data processing technologies are transversally interoperable in all sectors (commercial, informational, criminal…) and all applications (support, communication, prevention of future crime, investigation of committed crime…) could

threaten trust, privacy, anonymity and security. Full interoperability and free flow of personal data are not always desirable; interoperability should not just be considered as indispensable, certainly not as unquestionable.

Interoperability can entail an unlimited availability of personal data for any purpose. In fact, the concept of interoperability of personal data is based on unlimited availability of personal data. Interoperability may infringe upon the finality and purpose specification principles and erode the rights and guarantees offered by privacy and data protection law. Moreover, general availability of personal data for any private or public purpose seems to erode the basic fundamentals of data protection law: the purposes for which the data are available are often too broadly described (What is "state security", "terrorism", "a serious crime"?). Data can become available afterwards for *any* purpose. Interoperability of data and data processing mechanisms facilitates possible *function creep* (use of data for other purposes than originally envisaged).

Interoperability could contribute to the criminal use of ambient intelligence, for example, by sending viruses to objects in the network (interoperability opens the door for fast transmission and reproduction of a virus) or abusing data (interoperable data formats make data practical for any usage). Interoperability is thus not only a technological issue.

Awareness – already today – of the possible negative sides of interoperability should bring about a serious assessment of both law and technology *before* the market comes up with tools for interoperability. Legal initiatives in France (e.g., requiring interoperability of the iTunes music platform) and sanctions imposed by the European Commission (imposing interoperability of the Microsoft work group server operating system) indicate clearly that the need for interoperability is desired on a political and societal level.

In the Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 2005,[297] interoperability is defined as the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge". This is, however, a more technological definition: It "explicitly disconnects the technical and the legal/political dimensions from interoperability, assuming that the former are neutral and the latter can come into play later or elsewhere … Indeed, technological developments are not inevitable or neutral, which is *mutatis mutandis* also the case for technical interoperability. The sociology of sciences has shown that any technological artefact has gone through many small and major decisions that have moulded it and given it its actual form. Hence, the development of information technology is the result of micro politics in action. Technologies are thus interwoven with organisation, cultural values, institutions, legal regulation, social imagination, decisions and controversies, and, of course, also the other way round. Any denial of this hybrid nature of technology and society blocks the road toward a serious political, democratic, collective and legal assessment of technology. This means that technologies cannot be considered as *faits accomplis* or extra-political matters of fact."[298]

[297] Commission of the European Communities, Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM (2005) 597 final, Brussels, 24 November 2005.

[298] De Hert, P., & S. Gutwirth, "Interoperability of police databases: an accountable political choice", to be published in *International Review of Law Computers & Technology*, 2006; De Hert, P., "What are the risks

This way of proceeding has also been criticised by the European Data Protection Supervisor, according to whom this leads to justifying the ends by the means.[299]

Taking into account the need for interoperability, restrictions in the use and implementation of interoperability are required, amongst others based on the purpose specification and proportionality principles. To this extent, a distinction between the processing of data for public (enforcement) and private (support) purposes, may be absolutely necessary. Access to the databases by state enforcement agencies may be granted only on a case-by-case basis. Hereby, interoperability should not only be seen as a technical issue (solved by technical means) but also as a political, legal and economical issue (solved by legal, political and economical means). In addition, interoperability of the ambient intelligence system with third country systems that do not offer an adequate level of protection is very questionable.[300]

To achieve certain purposes, for which access to data has been granted, access to the *medium* carrying the information (e.g., a chip) may be sufficient, for example, when verifying one's identity. There should always be clarity as to what authorities are being granted access to data. In the case of deployment of centralised databases, a list of authorities that have access to the data should be promulgated in an adequate, official, freely and easily accessible publication.[301] Such clarity and transparency would contribute to security and trust, and protect against abuses in the use of databases.

Proportionality and purpose limitation principle

The proportionality and purpose limitation principles are already binding under existing data protection laws. The collection and exchange of data (including interoperability) should be proportional to the goals for which the data have been collected. It will not be easy to elaborate the principles of proportionality and purpose limitation in ambient intelligence; previously collected data may serve for later developed applications or discovered purposes. It often might occur that the creation and utilisation of databases can create additional benefits (which are thus additional purposes), e.g., in the case of profiling. Those other (derived) purposes should, as has been indicated in the opinion of the European Data Protection Supervisor, be treated as independent purposes for which all legal requirements must be fulfilled.[302]

---

and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection',* No. 1. ww.vub.ac.be/LSTS/pub/Dehert/006.pdf

[299] European Data Protection Supervisor (EDPS), *Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability* (COM (2005) 490 final), Brussels, 28 February 2006. http://www.edps.eu.int/legislation/Opinions_A/06-02-28_Opinion_availability_EN.pdf

[300] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004)835 final) *OJ C* 181/27, 23 July 2005, 13-29, sub 3.13. See also De Hert, P., "What are the risks and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection',* No. 1. www.vub.ac.be/LSTS/pub/Dehert/006.pdf

[301] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM (2004) 835 final, *Official Journal* C 181/27, 23 July 2005, sub 3.7, pp. 13-29.

[302] Idem, sub 3.2.

Technical aspects of system operation can have a great impact on the way a system works, and how the proportionality principles and purpose limitation principles are implemented since they can determine, e.g., if the access to the central database is necessary, or whether access to the chip or part of the data is possible and sufficient.

Biometrics

Biometric technology can be a useful tool for authentication and verification, or may even be considered as a privacy-enhancing technology. However, it can also constitute a threat to the fundamental rights and freedoms of the individual. Thus, specific safeguards should be put in place. Biometric safeguards have already been subject of reflection by European data protection authorities: the Article 29 Working Party stated that biometric data are in most cases personal data, so that data protection principles apply to processing of such data. [303]

The Article 29 Working Party brings special attention to the principle of proportionality and points out that it is not necessary (for the sake of authentication or verification) to store biometric data in central databases, but in the medium (e.g., a card) remaining in the control of the user.[304]

The creation and use of the centralised systems (centralised databases) should always be carefully assessed before its deployment, including prior checking by data protection authorities. In any case, all appropriate security measures should be put in place.

Framing biometrics is more than just deciding between central or local storage. Even storage of biometric data on a smart card should be accompanied by other regulatory measures that take the form of rights for the card-holders (to know what data and functions are on the card; to exclude certain data or information from being written onto the card; to reveal at discretion all or some data from the card; to remove specific data or information from the card).[305]

Biometric data should not be used as unique identifiers, mainly because biometric data still do not have sufficient accuracy.[306] Of course, this might be remedied in the progress of science and technological development. There remains, however, a second objection: using biometrics as the primary key will offer the possibility of merging different databases, which can open the doors for abuses (function creep).

---

[303] See Article 29 Data Protection Working Party, *Working document on biometrics* (12168/02/EN - WP 80), adopted on 1 August 2003, available through http://ec.europa.eu/justice_home/fsj/privacy/; Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, available through http://www.fidis.net [deliverables].

[304] See also De Hert, P., *Biometrics: legal issues and implications*, Background paper for the Institute of Prospective Technological Studies, EC – JRC, Sevilla, January 2005, p.13. Available at http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf.

[305] Neuwrit, K., *Report on the protection of personal data with regard to the use of smart cards,* Report of Council of Europe (2001), accessible through http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents, quoted by De Hert, P., *Biometrics: legal issues and implications, o.c.,* p. 26.

[306] Institute for Prospective Technological Studies (IPTS), *Biometrics at the frontiers: assessing the impact on Society*, Study commissioned by the LIBE committee of the European Parliament, EC – DG Joint Research Centre, Seville, February 2005.
http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf

European advisory bodies have considered the storage of raw data and the use of biometric data as a unique identifier. Generally speaking, since the raw data might contain more information than actually needed for certain finalities (including information not known at the moment of the collection, but revealed afterwards due to progress in science, e.g., health information related to biometric data), it should not be stored.[307] Other examples of opacity rules applied to biometrics might be: prohibitions on possible use for ordinary purposes of everyday life (e.g., for ordinary financial transactions); prohibitions on "strong" multi-modal biometrics (unless for high security applications)[308] for everyday activities, such as getting keys for hotel rooms or transactions at grocery stories; prohibitions against financial rewards to promote participation in biometric identification programs; prohibitions on non-encrypted processing and transmitting of biometric data.[309] Codes of conduct can be appropriate tools to further regulate the use of technology in the particular sectors.[310]

RFIDs

AmI will depend on profiling as well as authentication and identification technologies. To enable pervasive and ubiquitous communication between a person and his or her environment, both things and people will have to be traced and tracked. RFID seems to offer the technological means to implement such tracing and tracking. Like biometrics, RFID is an enabling technology for real-time monitoring and decision-making. Like biometrics, RFIDs can advance the development of AmI and provide many advantages for users, companies and consumers.[311]

Apparently no legislative action seems to be needed to support this developing technology. Market mechanisms are handling this. There is, however, a risk to the privacy interests of the individual and for a violation of the data protection principles, as CASPIAN and other privacy groups have stated. [312]

RFID use should be in accordance with privacy and data protection regulations. The Article 29 Working Party has already given some guidelines on the application of the principles of EU data protection legislation to RFID.[313] It stresses that the data protection

[307] European Data Protection Supervisor (EDPS), *Comments on the Communication of the Commission on interoperability of European databases*, 10 March 2006. http://www.edps.eu.int/legislation/Comments/06-03-10_Comments_interoperability_EN.pdf

[308] Biometrics, and especially multimodal biometrics, may increase the security of an application, and thus privacy as well. In its technical safeguards, the SWAMI consortium proposes use of multi-modal fusion of several less-privacy intrusive biometrics (e.g., fat, weight, height, gait, behavioural patterns) for everyday activities such as user-friendly authentication in mobile phones or authentication of car drivers. Such biometrics have low accuracy now, but as it is just emerging, such technology will most likely become more accurate later, and at the same time represent a lower threat to privacy than "strong" biometrics. For high-security applications, we recommend a combination of strong multi-modal biometrics with continuous unobtrusive authentication by less strong biometrics, provided that all modalities of the strong biometrics have good anti-spoofing capabilities. Use of biometrics should always be accompanied by adequate PETs.

[309] See De Hert, P., *Biometrics: legal issues and implications,* o.c., p. 25, and the literature quoted there.

[310] Article 29 Data Protection Working Party, *Working document on biometrics*.

[311] A description of RFID technologies and of usages can be found in Hildebrandt M. and J. Backhouse (eds.) *Descriptive analysis and inventory of profiling practices*, FIDIS (Future of Identity in the Information Society), Deliverable D7.2, June 2005, http://www.fidis.net.

[312] See e.g. Günther, Oliver and Sarah Spiekermann, "RFID and the Perception of Control: The Consumer's View", *Communications of the ACM*, Vol. 48, No. 9, 2005, pp. 73-76.

[313] Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology* (10107/05/EN - WP 105), 19 January 2005. Available through

principles (purpose limitation principle, data quality principle, conservation principle, etc…) must always be complied with when the RFID technology leads to processing of personal data in the sense of the data protection directive. [314]

As the Article 29 Working Party points out, the consumer should always be informed about the presence of both RFID tags and readers, as well as of the responsible controller, the purpose of the processing, whether data are stored and the means to access and rectify data. Here techniques of (visual) indication of activation would be necessary. The data subject would have to give his consent for using and gathering of the information for any specific purpose. The data subject should also be informed about what type of data are gathered and whether the data will be used by the third parties.

In AmI, those rights may create a great burden, both on the data subject, on the responsible data controller and on all data processors. Though adequate, simplified notices informing on the policy of the data processors would be welcome (e.g., using adequate pictograms or similar means). In our opinion, such information should always be provided to consumers when RFID technology is used, even if the tag does not contain personal data in itself.[315] The data subject should also be informed how to discard, disable or remove the tag. The right to disable the tag can relate to the consent principle of data protection, since the individual should always have the possibility to withdraw his consent.

The possibility to disable the tag should at least be present when the consent of the data subject is the sole legal ground of processing the data. Disabling the tag should not lead to any discrimination of the consumer (e.g., in terms of the guarantee conditions).

Technological and organisational measures (e.g., the design of RFID systems) are of crucial importance in ensuring that the data protection obligations are respected (privacy by design, e.g., by technologically blocking unauthorised access to the data). Thus, availability and compliance with privacy standards are of particular importance.[316]

---

http://ec.europa.eu/justice_home/fsj/privacy/

[314] The concept of "personal data" in the context of RFID technology is contested. WP 29 states: In assessing whether the collection of personal data through a specific application of RFID is covered by the data protection Directive, we must determine (a) the extent to which the data processed relates to an individual and, (b) whether such data concerns an individual who is identifiable or identified. Data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated. In assessing whether information concerns an identifiable person, one must apply Recital 26 of the data protection Directive which establishes that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." And further: "Finally, the use of RFID technology to track individual movements which, given the massive data aggregation and computer memory and processing capacity, are if not identified, identifiable, also triggers the application of the data protection Directive", Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, 10107/05/EN WP 105, 19 January 2005, point 4.1.

Still, such information on a tag can be an unique identifier enabling the profiling activities. See Kardasiadou, Z., and Z. Talidou, *Report on Legal Issues of RFID Technology*, LEGAL IST (Legal Issues for the Advancement of Information Society Technologies) Deliverable D15, 2006, p. 16.

[316] Some standards have already been adopted in the RFID domain. The International Organization for Standardization has developed sector-specific standards, as well as more generic standards. Some standards have also been developed by EPCglobal Ltd. (www.epcglobal.org), an industry-driven organisation, creating standards to connect servers containing information relating to items identified by EPC (Electronic Product Code) numbers.

It is recommended that in initiatives leading to standardisation of technical specifications, data protection concerns be reflected. Privacy assessment of each particular RFID application could be a legally binding obligation.[317]

Further research on the RFID technology and its privacy implications is recommended.[318] This research should also aim at determining whether any legislative action is needed to address the specific privacy concerns of RFID technology. However, further development of the codes of conducts and good practices is recommended.[319]

Data protection and profiling: a natural pair

Profiling is as old as life, because it is a kind of knowledge that unconsciously or consciously supports the behaviour of living beings, humans not excluded. It might well be that the insight that humans often 'intuitively know' something before they 'understand' it, can be explained by the role profiling spontaneously plays in our minds.

Thus, there is no reason to prohibit automated profiling and data mining concerning individuals with opacity rules. Profiling activities should in principle be ruled by transparency tools, namely tools that ensure the visibility, controllability and accountability of the profilers and the participation of those concerned. Our principled stance is similar to the one held in data protection: as a rule, the processing of personal data – collection, registration, and processing in the strict sense – is not prohibited but submitted to a number of conditions guaranteeing the visibility, controllability and accountability of the data controller and the participation of the data subjects.

Data protection rules apply to profiling techniques (at least in principle).[320] The collection and processing of traces surrounding the individual must be considered as processing of personal data in the sense of existing data protection legislation. Both individual and group profiling are dependent on such collection and processing of data generated by the activities of individuals. Without collecting and correlating such personal data, no profiling is thinkable. And that is precisely why, in legal terms, no profiling is thinkable outside data protection.

---

[317] Borking, J., "RFID Security, Data Protection & Privacy, Health and Safety Issues", presentation made during European Commission Consultation on RFID, Brussels, 17 May 2006.

[318] Such research is now carried out In the framework of the FIDIS programme and will lead to publication of a report on AmI, profiling and RFID (FIDIS Deliverable 7.7).

[319] An example of such (emerging) initiatives is the EPCglobal Ltd. guidelines regarding privacy in RFID technology, http://www.epcglobal.org/public_policy/public_policy_guidelines.html, and CDT (Centre for democracy and technology) Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology**,** Interim Draft, 1 May 2006, http://www.cdt.org/privacy/20060501rfid-best-practices.php. Though these are good examples of the involvement of stakeholders in the discussion, the results are not fully satisfactory. As a compromise between the different actors, the guidelines do not go far enough in protecting the interests of consumers. Sometimes the ambiguous wording of the guidelines (e.g., whether practicable…) may result in giving flexibility to industry to actually interpret the scope of their obligations.

[320] We add "at least in principle" because we are well aware of the huge practical difficulties of effectively enforcing and implementing data protection, more particularly in the field of profiling. See Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS (Future of Identity in the Information Society) Deliverable D7.3, August 2005. http://www.fidis.net. See also Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", to be published in M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen*, forthcoming, Springer Press, 2007. See also discussion on RFID above.

There is an ongoing debate in contemporary legal literature about the applicability of data protection to processing practices with data that is considered anonymous, viz. data that do not allow the identification of a specific individual.[321] This debate also has repercussions on the legal regime on profiling. Some contend that data protection rules do not allow processing practices that bring together data on certain individuals without trying to identify the said individual (in terms of physical location or name). Some contend that data protection rules do not apply to profiling practices that process data relating to non-identifiable persons (in the sense of the data protection directive). We hold that it is possible to interpret the European data protection rules in a broad manner covering *all* profiling practices,[322] but the courts will have the last word on this (and the courts have not spoken yet).

What is more important in this context is our belief that data protection should apply and that, when confusion in the application and interpretation of the legal instruments remains, they should be adapted as to make this possible. Profiling practices and the consequent personalisation of the ambient intelligence environment lead to an accumulation of power in the hands of those who control the profiles and should therefore be made transparent.

We are convinced that the principles of data protection are an appropriate starting point to cope with profiling in a democratic constitutional state as they do impose good practices. Nevertheless, while the default position of data protection is transparency ("Yes, you can process, but ..."), it does not exclude opacity rules ("No, you cannot process, unless…"). In relation to profiling, two examples of such rules are relevant. On the one hand, of course, there is the explicit prohibition against making and taking decisions affecting individuals solely on the basis of the automated application of a profile without human intervention (see art. 15 of the data protection directive).[323] This seems obvious because in such situation, probabilistic knowledge is applied to a real person. On the other hand, there is the (quintessential) purpose specification principle, which provides that the processing of personal data must meet specified, explicit and legitimate purposes. As a result, the competence to process is limited to well-defined goals, which implies that the processing of the same data for other incompatible aims is prohibited. Processing of personal data for different purposes should be kept separated. This, of course, substantially restricts the possibility to link different processing and databases for profiling or data mining objectives. The purpose specification principle is definitely at odds with the logics of

[321] We recall that *personal data* in the EU Data Protection Directive refers to "any information relating to an identified or identifiable natural person" (Article 1).

[322] De Hert, P., "European Data Protection and E-Commerce: Trust Enhancing?", in J.E.J. Prins, P.M.A. Ribbers, H.C.A. Van Tilborg, A.F.L. Veth & J.G.L. Van Der Wees (eds.), *Trust in Electronic Commerce*, Kluwer Law International, The Hague, 2002, pp. 190-199. See also Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", l.c.

[323] Article 15. Automated individual decisions. 1. Member States shall grant the right to every person 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. 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: (a) 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; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

interoperability and availability of personal data: the latter would imply that all thinkable databases can jointly be used for profiling purposes.[324] In other words, the fact that the applicable legal regime to profiling and data mining is data protection does not give a *carte blanche* to mine and compare personal data that were not meant to be connected.[325]

The European Data Protection Supervisor indicated in his Annual Report 2005 a number of processing operations that are likely to encompass specific risks to the rights and freedoms of data subjects, even if the processing does not occur upon sensitive data. This list relates to processing operations (a) of data relating to health and to suspected offences, offences, criminal convictions or security measures (b) intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct (c) allowing linkages, not provided for pursuant to national or Community legislation, between data processed for different purposes (d) for the purpose of excluding individuals from a right, benefit or contract.[326]

4.4.5 Specific recommendations regarding security

Software can be the tool for regulating one's behaviour by simply allowing or not allowing certain acts. Thus, technology constituting the "software code" can affect the architecture of the Internet (and thus potentially of AmI) and can provide effective means for enforcing the privacy of the individual. For example, cryptology might give many benefits: it could be used for pseudonymisation (e.g., encrypting IP addresses) and ensuring confidentiality of communication or commerce.[327]

Privacy-enhancing technologies can have an important role to play, but they need an adequate legal framework.

The directive on the legal protection of software[328] obliges Member States to provide appropriate remedies against a person committing any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical devices which may have been applied to protect a computer program. This mechanism aims to protect programs enforcing the intellectual property rights against circumvention.

Similar legal protection against circumvention of privacy-enhancing technologies could be legally foreseen.

Technology might go beyond what the law permits (for example, DRM prevents intellectual property infringements but at the same time might limit the rights of the lawful

[324] De Hert, P., "What are the risks and what guarantees need to be put in place in view of interoperability of police databases?", Standard Briefing Note 'JHA & Data Protection', No. 1, produced in January 2006 on behalf of the European Parliament, available through http://www.vub.ac.be/LSTS/

[325] Gutwirth, S. & P. De Hert, "Regulating profiling in a democratic constitutional state", to be published in M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen*, forthcoming, Springer Press, Berlin, 2007.

[326] European Data Protection Supervisor (EDPS), *Annual Report 2005*, pp. 22-23. http://www.edps.eu.int/publications/annual_report_en.htm.

[327] Leenes, Ronald and Bert-Jan Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, pp. 331-332

[328] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17/05/1991, pp. 0042 – 0046.

user). Negative side effects of such technologies should be eliminated. More generally, when introducing new technology on the market, manufacturers together with relevant stakeholders should undertake a privacy impact assessment. *Development of a participatory impact assessment procedure would allow stakeholders to quickly identify and react to any negative features of technology* (see below, where DRMs and intellectual property rights are discussed).

Empowering the individual

The European data protection directive imposes obligations on the data controller and gives rights to the data subject. It aims at giving the individual control over the collection and the processing of his data. In general, many provisions in the data protection directive have several weaknesses if confronted with the ambient intelligence environment. Principles of proportionality and fairness are relative and may lead to different assessments in similar situations; obtaining consent might be not feasible in the constant need for the collection and exchange of data; obtaining consent can be simply imposed by the stronger party. Individuals might not be able to exercise the right to consent, right to information, access or rectification of data due to the overflow of information. Thus, those rules might simply become unworkable in AmI. And even if workable (e.g., thanks to the help of the digital assistants), are they enough? Should we not try to look for an approach granting the individual even more control? Several projects have already considered such an approach and proposed decentralised identity and personal data management and the granting of property over personal information.

Decentralised identity (data) management

Several European projects are involved in research on identity management. They focus on the decentralised approach, where a user controls how much and what kind of information he or she wants to disclose. Identity management systems, while operating on a need-to-know basis, offer the user the possibility of acting under pseudonyms, under unlinkability or anonymously, if possible and desirable.

Among the other examples of such systems,[329] there are projects that base their logic on the assumption that the individual has the property over his data, and then use licensing schemes when a transfer of data occurs. Granting him property over the data[330] is seen as giving him control over the information and its usage in a "distribution chain". However, it is doubtful if in reality granting him property over the data will really empower the individual and give him a higher level of protection and control over his data. The property model also assumes that the data are disseminated under a contract. Thus, the question might arise whether the data protection directive should serve as a minimum standard and

[329] An overview of the existing identity management systems has been given by Bauer M., M. Meints and M. Hansen (eds.), *Structured Overview on Prototypes and Concepts of Identity Management Systems*, FIDIS (Future of Identity in the Information Society) Deliverable D3.1, September 2005, and Hildebrandt M. and J. Backhouse (eds.), *Descriptive analysis and inventory of profiling practices*, FIDIS Deliverable D7.2, June 2005, and Müller G. and S. Wohlgemuth (eds.), *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, May 2005. http://www.fidis.net

[330] See Lessig, L., *Code and other law of cyberspace*, Basic Books, New York, 1999, and Leenes, Ronald, and Bert-Jan Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, pp. 329. See also Samuelson, P., "Privacy As Intellectual Property?", *Stanford Law Review*, Vol. 52, 2000.

thus limit the freedom of contracts.[331] But as the SWAMI dark scenarios show, there exist many cases in which the individual will not be able to *freely* enter into a contract. Another question arises since *our* data are not always collected and used for commercial purposes. Even more, in most situations, the processing of personal data is a necessary condition for entering into a contractual relation (whereas the data protection directive states in Article 7 that data processing without the individual's consent to use of his personal data is legitimate when such processing is necessary for the performance of a contract). The most obvious example is the collection of data by police, social insurance and other public institutions. The individual will not always be free to give or not give his data away. The property model will not address these issues. It will also not stop the availability of the data via public means.[332]

A weakness of the property model is that it might lead to treating data only as economic assets, subject to the rules of the market. But the model's aim is different: the aim is to protect personal data, without making their processing and transfer impossible. Regarding data as property also does not address the issue of the profile knowledge derived from personal data. This knowledge is still the property of the owner or the licenser of the profile. The data-as-property option also seems to ignore the new and increasingly invisible means of data collection, such as RFIDs, cameras or on-line data collection methods.

Having said that, it could be concluded that discussing the issue of whether personal data should become the individual's property or not does not solve the core problem. On the one hand, treating data as property may lead to a too high level of protection of personal information, which would conflict with the extensive processing needs of AmI. On the other hand, it would, by default, turn personal data into a freely negotiable asset, no longer ruled by data protection, but left to market mechanisms and consent of the data subjects (more often than not to the detriment of the latter). Finally, the data-as-property option loses its relevance in the light of a focus upon anonymisation and pseudonymisation of data processed in AmI applications.

The PRIME consortium proposes identity management systems controlled by data subjects.[333] It aims to enable individuals to negotiate with service providers the disclosure of personal data according to the conditions defined. Such agreement would constitute a contract.[334] An intelligent agent could undertake the management on the user side. This solution is based on the data minimisation principle and on the current state of legislation. It proposes the enforcement of (some) current data protection and privacy laws. It seems to be more designed for the needs of the world today than for the future AmI. It could still be possible that the user is forced to disclose more information than he or she wishes, because he or she is the weaker party in the negotiation; he or she needs the service.

The FIDIS consortium also proposed a preliminary vision of decentralised identity management. This vision seems to go a bit further than the PRIME proposal. It foresees

[331] However, currently this is not the case. The weaker party in the contract is now protected by the general principles of law. Prins, J.E.J., "The Propertization of Personal Data and Identities", *Electronic Journal of Comparative Law*, vol. 8.3, October 2004. http://www.ejcl.org/
[332] Idem.
[333] Hansen, Marit and Henry Krasemann (eds.), *Privacy and Identity Management for Europe*, PRIME White Paper, Deliverable D 15.1.d, 18 July 2005. Available through http://www.prime-project.eu.org/.
[334] Ibid., p. 7.

that the user profiles are stored with the device of a user, and preferences relevant for a particular service are (temporarily) communicated to the service provider for the purpose of a single service. The communication of the profile does not have to imply disclosure of one's identity. If there is information extracted from the behaviour of the user, it is transferred by the ambient intelligent device back to the user, thus updating his profile.[335] Thus, some level of exchange of knowledge is foreseen in this model, which can be very important for the data subject's right to information.

A legal framework for such sharing of the knowledge (from an AmI-generated profile) needs to be developed, as well as legal protection of the technical solution enabling such information management. Such schemes rely on automated protocols for the policy negotiations. The automated schemes imply that the consent of the data subject is also organised by automatic means. It is desirable to clearly foresee a legal framework dealing with the situation wherein the explicit consent of the data subject for each collection of data is replaced by a "consent" given by an intelligent agents.

In such automated models, privacy policies following the data might be also envisaged. Such "sticky" policies, attached to personal data, would provide for clear information and indication towards data processors and controllers which privacy policy applies to the data concerned.[336] They could facilitate the auditing and self-auditing of the lawfulness of the data processing by data controllers.[337] *In any event, research in this direction is desirable.*

Since AmI is also a mobile environment, there is a need to develop identity management systems addressing the special requirements of mobile networks. The FIDIS consortium has done research on the subject and prepared a technical survey of mobile identity management. It has identified some special challenges and threats to privacy in the case of mobile networks and made certain recommendations:

- Location information and device characteristics both should be protected.
- Ease of use of the mobile identity management tools and simplified languages and interfaces for non-experts should be enhanced.
- A verifiable link between the user and his digital identity has to be ensured. Accordingly, privacy should also be protected in peer-to-peer relationships.[338]

4.4.6 Specific recommendations regarding consumer protection law

The importance of consumer protection will grow in ambient intelligence, because of the likelihood that consumers will become more dependent on on-line products and services, and because product and service providers will strengthen their bargaining position through an increasing information asymmetry. Without the constraints of law, ambient

[335] Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS (Future of Identity in the Information Society) Deliverable D7.3, August 2005, p. 32. http://www.fidis.net.

[336] Meints, M., "AmI - The European Perspective on Data Protection Legislation and Privacy Policies", Presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006.

[337] For example, such an approach was adopted by the PAW project (Privacy in an Ambient World), which has developed the language enabling the distribution of the data in a decentralised architecture, with the usage policies attached to the data, informing what kind of usage has been licensed to the particular actor (licensee). Enforcement relies on auditing. http://www.cs.ru.nl/paw/results.html

[338] Müller G. and S. Wohlgemuth (eds.), *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, May 2005. http://www.fidis.net.

intelligence service providers easily obtain a position to dictate the conditions of participation in new environments. Consumer protection should find the proper balance in AmI.

Consumer protection law defines the obligations of the producers and the rights of consumer and consists of a set of rules limiting the freedom to contract, for the benefit of the consumer. Consumer protection law plays a role of its own, but can support the protection of privacy and data protection rights.[339]

The basis for the European framework for consumer protection rules can be found in Article 153 of the EC Treaty: "In order to promote the interests of consumers and to ensure a high level of consumer protection, the community shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests."

Consumer protection at European level is provided by (amongst others) Directive 93/13 on unfair terms in consumer contracts[340] and Directive 97/7 on consumer protection in respect of distance contracts[341], and product directives (discussed below). Directive 93/13 and Directive 97/7 were both extensively discussed in our previous deliverables.[342] In many respects, those rules are not fitted to AmI and they need to be re-adapted. This especially relates to extending the scope of protection of those directives, thereby making sure that all services and electronic means of communications and trading are covered (including those services on the World Wide Web not currently covered by the distance selling directive).[343]

Contracts could be concluded by intelligent agents

Due to the increasing complexity of on-line services, and due to the possibility of information overflow, it seems necessary to find legal ways to assess and recognise contracts made through the intervention of intelligent agents. Is the legal system flexible enough to endorse this? Moreover, the same should apply to the privacy policies and to the consent of individuals for the collection of data (because, in identity management systems, intelligent agents will decide what data are to be disclosed to whom).

Here is a challenge: how to technologically implement negotiability of contracts and the framework of binding law in electronic, machine-readable form?

[339] Although we focus here on the issue of the services, in an AmI environment, it can be difficult to distinguish between a product and a service. Though it is often difficult to draw the line between the two, different legal regimes apply. Product liability issues are discussed below.
[340] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *Official Journal* L 095, 21/04/1993, pp. 29 – 34.
[341] 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, *Official Journal* L 144, 04/06/1997, pp. 0019 – 0027.
[342] Friedewald M., E. Vildjiounatie and D. Wright (eds.), *The brave new world of ambient intelligence: A state-of-the-art review,* SWAMI Deliverable D 1, July 2005, p.156.
[343] Henderson, K., and A. Poulter, "The Distance Selling Directive: Points for Further Revision", *International Review for Law Computers & Technology*, Vol. 16 no. 3, 2002, pp. 289-300.

Unfair privacy policies

Suppliers should not be allowed to set up privacy conditions which are manifestly not in compliance with the generally applicable privacy rules and which disadvantage the customer.

Data protection legislation and consumer protection law could constitute the minimum (or default) privacy protection level. Similar rules as those currently applicable under the consumer protection of Directive 93/13 on unfair terms in consumer contracts could apply. Mandatory rules of consumer protection require, *inter alia,* that contracts be drafted in plain, intelligible language; that the consumer should be given an opportunity to examine all terms; that – in case of doubt – the interpretation that is most favourable to the consumer prevails.

Suppliers should not be allowed to unfairly limit their liability for security problems in the service they provide to the consumer.

In this respect, more attention could be given to a judgment of the Court of First Instance of Nanterre (France) in 2004 in which the online subscriber contract of AOL France was declared illegal in that it contained not less than 31 abusive clauses in its standard contractual terms (many of which infringed consumer protection law).[344]

Information to the consumer

The directive on unfair terms in consumer contracts and the directive on consumer protection in respect of distance contracts provide a broad right to information for the consumer. *It should be clearly stated that it is sufficient to dispense such information in electronic form (machine and human readable)*[345], especially in view of the large amount of information directed towards consumers that would have to be managed by intelligent agents.

An increasing number of service providers will be involved in AmI services and it cannot be feasible to provide the required information about all of them. The solution may be a requirement to provide such information only about the service provider to whom the consumer directly pays and who is responsible towards the consumer (joint liability would apply; for liability issues, see below).

Right to withdrawal

The right to withdrawal, foreseen by the Directive 97/7 on consumer protection with respect to distance contracts, may not apply (unless otherwise agreed) to contracts in which (a) the provision of services has begun with the consumer's agreement before the end of the seven-working-day period and (b) goods have been made to the consumer's specifications

[344] Tribunal de grande instance de Nanterre, 2 June 2004 (*UFC Que Choisir* v. *AOL Bertelsmann Online France*), available at http://www.legalis.net/jurisprudence-decision.php3?id_article=1211. For an English analysis, see Naylor, David, & Cyril Ritter, "B2C in Europe and Avoiding Contractual Liability: Why Businesses with European Operations Should Review their Customer Contracts Now", 15 September 2004. http://www.droit-technologie.org

[345] Currently, insofar as it is not received on a permanent medium, consumers must also receive written notice in good time of the information necessary for proper performance of the contract.

or clearly personalised or which, by their nature, cannot be returned or are liable to deteriorate or expire rapidly.

In an AmI world, services will be provided instantly and will be increasingly personalised. This implies that the right of withdrawal in many cases will become inapplicable. New solutions should be developed to address this problem.

Temporary accounts

In AmI, payments will often occur automatically, at the moment of ordering or even offering the service.

Temporary accounts, administered by trusted third parties, could temporarily store money paid by a consumer to a product or service provider. This can support consumer protection and enforcement, in particular with respect to fraud and for effectively exercising the right of withdrawal. This would be welcome for services that are offered to consumers in the EU by service providers located in third countries, as enforcement of consumer protection rights is likely to be less effective in such situations.

Group litigation and consumer claims

The possibility of group consumer litigation[346] can increase the level of law enforcement and, especially, enforcement of consumer protection law. Often an individual claim does not represent an important economic value, thus, individuals are discouraged from making efforts to enforce their rights.

Launching collective claims or similar actions would increase the effective power against service providers. A similar solution is now available at European level in the case of injunctions.

Bodies or organisations with a legitimate interest in ensuring that the collective interests of consumers are protected *can* institute proceedings before courts or competent administrative authorities and seek termination of any behaviour adversely affecting consumer protection and which is defined by law as illegal.[347,] However, as far as actions for damages are concerned, issues such as the form and availability of the group litigation,

[346] Group litigation is a broad term which captures collective claims (single claims brought on behalf of a group of identified or identifiable individuals), representative actions (single claims brought on behalf of a group of identified individuals by, e.g., a consumer interest association), class action (one party or group of parties may sue as representatives of a larger class of unidentified individuals), among others. These definitions as well as the procedural shape of such claims vary in different Member States. Waelbroeck D., D. Slater and G. Even-Shoshan G [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, pp. 44.
http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.html. The SWAMI consortium abstains from designating one of those forms as adequate. Instead, we recommend to the adequate authority to further study the issue, however, which points to the controversial character of class actions on European grounds and thus proposes to focus on other possible forms.

[347] Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 On injunctions for the protection of consumers' interests, *Official Journal* L 166, 11/06/1998, pp. 51 – 55.

as part of procedural law are regulated by the national laws of the Member States. The possibility to bring such a claim is restricted to a small number of states.[348]

4.4.7 Specific recommendations regarding electronic commerce

The scope of the e-commerce directive

The e-commerce directive[349] aims to provide a common framework for information society services in the Member States of the EU (see SWAMI deliverable 1). An important feature of the directive is that it also applies to the legal persons. Similar to the consumer protection legislature, the directive foresees an obligation to provide certain information to customers. In view of the increasing number of service providers, it may not be feasible to provide information about all of them. *Providing information about the service provider whom the customer pays directly and who is responsible towards him could be a solution to the problem of the proliferating number of service providers (joint liability may also apply here). There is also a need to conclude contracts exclusively via intelligent agents. Intelligent agents will also manage the information, which, according to law, has to be provided to consumers. This information should enable an individual to enforce his rights in court, if necessary. Thus, the directive should be updated to include the possibility of concluding contracts by electronic means (including reference to intelligent agents). In any updating of the directive, there is also a need to facilitate the usage of pseudonyms, trusted third parties and credentials in electronic commerce.*

Unsolicited communication (spam)

Unsolicited commercial communication is an undesirable phenomenon in cyberspace. It constitutes a large portion of traffic on the Internet, using its resources (bandwidth, storage capacity) and forcing Internet providers and users to adopt organisational measures to fight it (by filtering and blocking spam). Spam can also constitute a security threat.[350] The SWAMI dark scenarios show that spam may become an even more serious problem than it is today. [351] An increase in the volume of spam can be expected because of the emergence of new means of electronic communication. Zero-cost models for e-mail services encourage these practices, and similar problems may be expected when mobile services pick up a zero-cost or flat-fee model.

As we become increasingly dependent on electronic communication – ambient intelligence presupposes that we are almost constantly on-line – we become more vulnerable to spam. In the example from the first SWAMI dark scenario, spamming may cause irritation and

---

[348] Belgian law provides that in certain circumstances associations can bring collective damage action or action for several individual damages. Waelbroeck D., D. Slater and G. Even-Shoshan [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, pp. 44-47.
http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.html

[349] 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"), *Official Journal* L 178, 17/07/2000, pp. 0001 – 0016.

[350] Sorkin, David E., "Technical and Legal Approaches to Unsolicited Electronic Mail", *University of San Francisco Law Review*, Vol. 35, 2001, p. 336 and following.

[351] Punie, Y., S. Delaitre, I. Maghiros & D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities,* SWAMI Deliverable D 2, November 2005, Scenario 1 situation 2, p. 18 and p. 91

make the individual reluctant to use ambient intelligence. Fighting spam may well demand even more resources than it does today new methods of spamming – such as highly personalised and location-based advertising – emerge.

Currently, many legal acts throughout the world penalise unsolicited communication, but without much success. The Privacy and Electronic Communication Directive 2002[352] provides for an opt-in regime, applicable in the instance of commercial communication, thus inherently prohibiting unsolicited marketing.[353] Electronic communications are, however, defined as "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a 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."[354] The communications need to have a commercial content in order to fall under the opt-in regulation of Directive 2002/58/EC.[355]

Consequently, this directive may not cover unsolicited, location-based advertisements with a commercial content that are broadcast to a group of people ("the public"). The impact of this exception cannot be addressed yet since location-based services are still in infancy.

A broad interpretation of electronic communications is necessary (the directive is technology-neutral). Considering any unsolicited electronic communication as spam, regardless of the content and regardless of the technological means, would offer protection that is adequate in ambient intelligence environments in which digital communications between people (and service providers) will exceed physical conversations and communications.[356]

4.4.8 Specific recommendation regarding liability law

General

Civil damages address a harm already done, and compensate for damages sustained. Effective civil liability rules might actually form one of the biggest incentives for all actors involved to adhere to the obligations envisaged by law. One could establish liability for breach of contract, or on the basis of the general tort rules. To succeed in court, one has to prove the damage, the causal link and the fault. Liability can be established for any

[352] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) *Official Journal* L 201, 31/07/2002, pp. 37- 47.
[353] Andrews, S., *Privacy and human rights 2002*, produced by the Electronic Privacy Information Center (EPIC), Washington D.C. and *Privacy International*, London, 2002, p.12.
http://www.privacyinternational.org/survey/phr2002/
[354] Article 2 (d) of Directive 2002/58/EC.
[355] Recital 40 states, "Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient."
[356] Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", *op.cit*; Schreurs, W., "Spam en electronische reclame [Spam and electronic communication]", *Nieuw Juridisch Weekblad,* 2003-48, pp. 1174 - 1185.

damages sustained, as far as the conditions of liability are proven and so long as liability is not excluded (as in the case of some situations in which intermediary service providers are involved[357]). However, in AmI, to establish such proof can be extremely difficult.

As we have seen in SWAMI's dark scenarios, each action is very complex, with a multiplicity of actors involved, and intelligent agents acting for service providers often undertake the action or decision causing the damage. Who is then to blame? How easy will it be to establish causation in a case where the system itself generates the information and undertake the actions? How will the individual deal with such problems? The individual who is able to obtain damages addressing his harm in an efficient and quick way will have the incentive to actually take an action against the infringer, thus raising the level of overall enforcement of the law. Such an effect would be very desirable, especially since no state nor any enforcement agency is actually capable of providing a sufficient level of control and/or enforcement of the legal rules.

The liability provisions of the e-commerce directive can become problematic. The scope of the liability exceptions under the directive is not clear. The directive requires ISPs to take down the content if they obtain knowledge on the infringing character of the content (notice and take down procedure). However, the lack of a so-called "put back" procedure (allowing content providers whose content has been wrongfully alleged as illegal, to re-publish it on the Internet) or the verification of take-down notices by third parties is said to possibly infringe the freedom of speech.[358]

It is recommended that the liability rules be strengthened and that consideration be given to means that can facilitate their effectiveness.

The following paragraphs present a short discussion on these issues. First, we examine the problems related to the establishment of liability for breach of privacy. Then we move to the issues of joint liability and strict liability: these may help to establish liability. Then a possible procedural enhancement for the claimant is discussed, which represents a reversal of the burden of proof. Revoking the liability of certification service providers is given as an illustration.

Liability for infringement of the privacy law

We need to further examine the specific rules on liability for infringement of privacy and data protection law, including security infringements. Currently, the right to remedy in such circumstances is based on the general liability (tort) rules. Despite the fact that

[357] Articles 12 to 15 of the 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") *Official Journal* L 178, 17/07/2000, pp. 1-16. The Directive provides for exceptions to the liability for Intermediary Service Providers (ISPs) under certain conditions. In the case of hosting, for example, a 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.

[358] See Sutter Gavin, "'Don't Shoot the Messenger?' The UK and Online Intermediary Liability", *International Review of Law Computers & Technology*, Vol. 17 No.1, 2003, pp. 73-84; Julia-Barcelo, R., and K. J. Koelman, "Intermediary Liability in the E- commerce Directive: So far so Good, But It's not Enough", *Computer Law and Security Report*, Vol. 16, No. 4, 2000, pp. 231-239.

meeting the general tort law preconditions (damage, causality and fault) can be very difficult, it could also be problematic to determine the scope of liability for privacy breach or security infringement.

The data protection directive refers explicitly to liability issues stating that an immediate compensation mechanism shall be developed in case of liability for an automated decision based on inadequate profiles and refusal of access. This mechanism may provide for a compensation scheme that does not require the satisfaction of the normal tort conditions. The directive also puts forward 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.[359] Still, unlawful processing would have to be proven first, which in many cases might be problematic (Was the collection of data proportional? fair? Such terms are very relative.). Moreover, the individual would have to actually sustain and prove the damage caused to him, and in some cases of the unlawful processing of data, damage does not have to be imminent or easily assessable (Is there a damage? What is the damage if the data were unlawfully collected and used for the building of a group profile, but there was no consequences (yet) of such processing directed towards a particular data subject?). Or should we understand this provision to mean that any act of unlawful data processing gives the right to damages, even if no (imminent and measurable) damage is sustained? Future developments and future case law should clarify these issues.

Opacity instruments, as discussed above, aiming to prohibit the interference into one's privacy can help to provide some clarity as to the scope of the liability. In addition, guidelines and interpretations on liability would be generally welcome, as well as standards for safety measures, to provide for greater clarity and thus greater legal certainty for both users and undertakings.

Joint and several liability

As already mentioned, in nearly every situation regarding consumer relationships, the factual situation might be very complex (e.g., in case of data mismatch and access refusal, the client is faced with a problem caused by a complex technological system, which has been constructed by the joint efforts of several actors). It can be troublesome for a user to point at the party who is actually responsible for the damages caused, especially if he or she does not know which parties were actually involved in the service and/or software creation and delivery.

Henceforth, the user should be enabled to point at and request compensation from the service provider with whom he or she had direct contact in the process of the service. Joint and several liability (with the right to redress) should be the default rule in the case of the providers of AmI services, software, hardware or other products, both in contractual and extra contractual liability cases. Complexity of the actions and multiplicity of actors justifies such a position.[360] Moreover, this recommendation should be supplemented by the consumer protection recommendation requiring the provision of consumer information by the service or product provider having the closest connection with the consumer, as well as the provision of information about the individual privacy rights (see above) in a way that would enable the individual to detect a privacy infringement and giving more chances to

[359] Article 23 of the data protection directive.
[360] Joint and several liability is already foreseen in the product liability directive.

prove it in a court. It follows that there is a need to consider the liability regime together with other provisions of law.

Strict liability

The product liability directive[361] provides for a liability without fault (strict liability).[362] As the recital to the Directive states, strict liability shall be seen as "the sole means of adequately solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production." We should keep this reasoning in mind since it seems even more adequate when thinking about the liability issues in AmI.

The AmI environment is one of high technical complexity, both in terms of the services offered and the software making them operational. In fact, most of the "products" offered in this environment will consist of software-based, highly personalised services. We should then think about adjusting the liability rules to such an environment. If it is difficult to distinguish between hardware and software from a technological perspective, why should we draw such a distinction from a legal perspective?[363] *An explicit provision providing for strict liability for software can be considered.*[364] Nevertheless, such a proposal is regarded as controversial. It is said to threaten industry. Since, in the opinion of the computer specialists, the software is never defect-free, the strict liability would expose software producers unfairly to the damages claims. Thus, the degree of required safety of the programs is a policy decision.[365] Strict liability could also impede innovation, especially the innovation of new, experimental and life-saving applications.[366] Others argue that strict liability might increase software quality by making producers more diligent, especially, in properly testing the product.[367]

Despite these policy considerations, there are some legal questions about the applicability of strict liability to software. The first issue to answer is whether the software can be regarded as "goods" or "products" and whether they fall under the strict liability regime.[368]

---

[361] 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, *Official Journal* L 210, 07/08/1985, pp.29 –33.

[362] A strict product liability regime based on the directive is the basis of the claims under the general tort regime. See Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", *Netherlands Comparative Law Association*, 2002, pp. 75-79. http://www.ejcl.org/64/art64-6.html.

[363] Hilty, Lorenz, et al, *The Precautionary Principle in the Information Society, Effects of Pervasive Computing on Health and Environment*, Report of the Centre for Technology Assessment, February 2005, p. 269.

[364] In such a case, the intelligent software agent's failure and the PET's failure might be covered by the strict liability regime. Special derogation for PETs could be envisaged.

[365] Alheit, K., "The applicability of the EU Product Liability Directive to Software", *The Comparative and International Law Journal of South Africa*, Vol. 3, no 2, 2001, p. 204.

[366] Singsangob A., *Computer Software and Information Licensing in Emerging Markets, The Need for a Viable Legal Framework*, Aspen Publishers, 2003, p. 113.

[367] Desai, M.S., J. Oghen and T.C. Richards, "Information Technology Litigation and Software Failure", *The Journal of Information, Law & Technology*, 2002 (2).
http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/desai/. Compare with coments on softwere testing under 2.3. and 4.2.6.

[368] Similar discussion takes place in the US. It seems that, despite the fact that the issue is not clearly stated, there is a tendency to regard software as a good, especially if the parties to the contract intended to treat it as such (as opposed to an information service). See Singsangob A., *Computer Software and Information Licensing in Emerging Markets, The Need for a Viable Legal Framework*, Aspen Publishers , 2003, p. 113.

In fact, the answer to that question depends on the national laws relating to those issues and implementing the directive. The directive applies to products defined as all movables[369], which might suggest that it refers to goods having a tangible medium. Software not incorporated into the tangible medium (available on-line) will not satisfy such a definition. There are a growing number of devices (products) with embedded software (e.g., washing machines, microwaves, possibly RFIDs), which fall under the regime of the directive today.[370] Such a tendency will continue, though the software application will be increasingly crucial for the proper functioning of the products themselves, services and whole environments (smart car, smart home). Should the distinction between the two regimes remain?

Strict liability is limited to death or personal injury, or damage to property intended for private use.[371] The damage relating to the product itself, to the product used in the course of business and the economic loss, will not be remedied under the directive.[372] Currently, defective software is most likely to cause financial loss only, thus the injured party would not be able to rely on provisions of the directive in seeking redress. However, even now in some life-saving applications, personal injury dangers can emerge. Such will also be the case in the AmI world (see, for example, the first and second SWAMI dark scenarios in which software failures cause accidents, property damage and personal injury) so the importance and applicability of the product liability directive will grow. The increasing dependence on software applications in everyday life, the increasing danger of sustaining personal injury due to a software failure and, thus, the growing concerns of consumers justify strengthening the software liability regime.

However, the directive allows for a state-of-the-art defence. Under this defence, a producer is not liable if the state of scientific and technical knowledge at the time the product was put into circulation was not such that the existence of the defect would be discovered. It has been argued that the availability of such a defence (Member States have the discretion whether to retain it in the national laws or not[373]) will always be possible since, due to the complexity of "code", software will never be defect free.[374]

The above-mentioned policy arguments as well as the legal arguments show the difficulty in broadening the scope of the strict liability directive to include software, but they might also point to an alternative solution. Reversal of the burden of proof might be a more adequate solution. Policy-makers should investigate which solution is best.

As mentioned, it is often difficult to distinguish software from hardware: both are necessary and interdependent to provide a certain functionality. Similarly, it may be difficult to draw the line between software and services. Transfer of information via

[369] Article 2 of the Directive.
[370] Reed, Ch., and A. Welterveden, "Liability", in Ch. Reed and J. Angel (eds.), *ComputerLaw*, London 2000, p. 99.
[371] Article 9 of the Product Liability Directive.
[372] Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", *Netherlands Comparative Law Association*, 2002, p. 82, http://www.ejcl.org/64/art64-6.html
[373] Article 15(1)(b) of the Product Liability Directive.
[374] Alheit, K., "The applicability of the EU Product Liability Directive to Software", *The Comparative and International Law Journal of South Africa*, Vol. 3, no 2, 2001, p. 204.

electronic signals (e.g., downloaded software) could be regarded as a service.[375] Some courts might also be willing to distinguish between mass-market software and software produced as an individual product (on demand). AmI is a highly personalised environment where the software-based services will surround the individual, thus the tendency to regard software as a service could increase.

Strict liability currently does not apply to services. Service liability is regulated by national laws.[376] Extending such provision to services can have far-reaching consequences, not only in the ICT field. The AmI environment will need the innovation and creativity of service providers; therefore one should refrain from creating a framework discouraging them from taking risks. However, some procedural rules could help service receivers (consumers), but without upsetting an equitable balance. The consumer, usually the weaker party in a conflict with the provider, often has difficulty proving damage caused to him. Reversing the burden of proof might facilitate such proof (see below). Most national laws seem to provide a similar solution.[377]

Since national law regulates the issue of service liability, differences between national regulations might lead to differences in the level of protection. The lack of a coherent legal framework for service liability in Europe is regrettable. Learning from the differences and similarities between the different national legal regimes, as indicated in the Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services,[378] is the first step in remedying such a situation.

Procedural enhancement of the claimant in liability actions

One of the biggest problems in liability actions is the issue of proof. In tort cases, it is difficult to prove the damage, fault and causal link. This will become even more problematic in an AmI future when users will increasingly depend on services, but not know the whole complexity behind the service delivery. In an AmI world, information will often be collected without the user noticing it and decisions often made without the user's knowledge. The complexity of the whole AmI environment creates asymmetries in information flow. While users are transparent to their service provider or other contractors, the reverse is often not the case. Often the information asymmetry makes it impossible for users to prove the fault or the causal link between the harmful event and the damage. However, once the damage is done, one should have the means to enforce one's right and receive compensation. *Thus, some procedural enhancement of the user's position seems necessary.*

[375] The OECD has treated software downloads as a service for the VAT and custom duties purposes; see Henderson, K., and A. Poulter, "The Distance Selling Directive: Points for Further Revision", *International Review for Law Computers & Technology*, Vol. 16 no. 3, 2002, p. 289-300

[376] As a basis for liability, the contractual liability or the fault-based tort liability applies. See Giensen, I., and M.B.M. Loos, *l.c.*as well as Magnus, U., and H.W. Micklitz, *Comparative Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services*: A study commissioned by the European Commission, Final Report, Part D: The Comparative Part, April 2004, p. 62.
http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf

[377] Magnus, U., and H.W. Micklitz, p. 8.

[378] Magnus, U., and H.W. Micklitz, p. 8.

Reversing the burden of proof

The individual will never have an adequate insight into the complexity of service delivery or data processing. The lack of knowledge and access to information can often place him in a disadvantageous position. *In many instances, reversing the burden of proof could remedy the inequality of the parties in a proceeding.* Thus, instead of the individual struggling to prove the elements of a claim and the liability of the service provider/data processor, the service providers would be obliged to prove otherwise. In many circumstances, the legal provisions granting the right to remedy might remain without effects, since the liability of the defendant is too difficult or impossible to prove. While reversing the burden of proof, service suppliers[379] are still able to defend their position and demonstrate that, for example, they have not neglected any means of precaution and thus they are not at fault. Reversing the burden of proof is less invasive than the strict liability rules, when the issue of fault is simply not taken into consideration.

Such a solution has been adopted in the field of the antidiscrimination and intellectual property laws, as well as in national tort systems.[380]

The technology could potentially remedy the information asymmetry between users and AmI service suppliers or data processors. The latter could have an obligation to inform consumers what data are processed, how and when and what is the aim of such activities (thus actually fulfilling their obligations under the data protection directive). This information could be stored and managed by an intelligent agent on behalf of the user, who is not able to deal with such information flow. However, the user would have the possibility to use such information to enforce his rights (e.g., to prove causation). Other technological solutions (e.g., watermarking) could also help the user prove his case in court.

Electronic signatures

Directive 1999/93/EC on the community framework for electronic signatures[381] establishes the framework for the liability of certification service providers for, *inter alia,* the accuracy and completeness of the certificate. The certification service provider is liable for damage caused by non-compliance with obligations imposed by the directive[382], unless he proves he did not act negligently. Such rules constitute an exception to the general liability regime, and aim to facilitate use of pseudonyms in electronic commerce. In fact, they

[379] Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", Netherlands Comparative Law Association, 2002. http://www.ejcl.org/64/art64-6.html

[380] Magnus, U., and H.W. Micklitz, *Comparative Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services*: A study commissioned by the European Commission, Final Report, April 2004.
http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportabc_en.pdf
http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf

[381] On issues relating to digital signatures, see Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005. http://www.fidis.net. See also Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures *Official Journal* L 013, 19/01/2000, pp. 0012-002. For commentary on the directive, see Friedewald, M., E. Vildjiounatie and D. Wright (eds.), *The brave new world of ambient intelligence: A state-of-the-art review*, SWAMI Deliverable D 1, July 2005, p. 167.

[382] For example, the service provider is liable for the inaccuracy or incompleteness of the information contained in the certificate at the tame the certificate was issued.

provide for stricter liability for service providers by reversing the burden of proof. It is an example of the solution the SWAMI consortium would propose for ICT service liability.

The liability rules described above seem sufficient as a legal framework for qualified digital signatures. The general tort rules apply in relation to liability in all other cases (other than qualified signatures).

Consumer claims and fixed damages

In many cases, the damage sustained by the individual will be difficult to assess in terms of the economic value or too small to actually provide an incentive to bring an action to court. However, acts causing such damage can have overall negative effects. Spam could be a good example. *Fixed damages, similar to the ones used in the US, or punitive damages could remedy such problems (some US state laws provide for fixed damages such as US$200 for each unsolicited communication without the victim needing to prove such damage). They would also provide clarity as to the sanctions or damages expected and could possibly have a deterrent effect.* The national laws of each Member State currently regulate availability of punitive damages; a limited number of countries seem to provide for punitive and exemplary damages in their tort systems.[383]

Actions allowing consolidation of the small claims of individuals could be also examined (i.e., group consumer actions).

4.4.9 Specific recommendation regarding equality law

What is non- discrimination law?

The scope of non-discrimination law is broad and well established.[384] Non-discrimination provisions have a general character and prohibit using some of the characteristics of people (sex, race, colour of skin, nationality, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of national minority, property, age, disability or sexual orientation[385]) in decision-making.[386] The general character of non-discrimination law ensures its broad application. This is its big potential. It will apply to AmI decisions based on a big amount of data (so possibly always containing certain sensitive characteristics, as mentioned above), including automated decisions. It will not, however, apply to use of such data for other purposes (collecting the data, profiling). Thus, non-discrimination law will not have the potential to regulate the flow of data – which today is the role of data protection legislation, but can regulate and forbid the unlawful usage of the data processed (e.g., in making decisions or undertaking other actions on the basis of certain characteristics of the data subjects). This makes the

[383] There are also not enough sources to state if they would apply in anti-spam cases. Available sources refers here to antitrust claims. Waelbroeck D., D. Slater and G. Even-Shoshan [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, pp. 44-47.
http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.htm

[384] Friedewald M., E. Vildjiounaite and D. Wright (eds.), *The brave new world of ambient intelligence: A state-of-the-art review,* SWAMI Deliverable D 1, July 2005, p.174, contains an overview of non-discrimination law.

[385] Charter of Fundamental Rights of the European Union, articles 21 and 23

[386] Custers, B., *The Power of Knowledge, Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen, 2004, pp. 164-165

non-discrimination law of increasing importance for AmI (as already discussed, in an AmI environment, we might not be able to control the flow and amount of the information actually needed by AmI, thus we should build in safeguards against its abuses). The *creation* itself of profiles does not fall under the non-discrimination law[387] (potential use), but decisions based on profiling (including group profiling based on anonymous data) which affects the individual might provide the grounds for application of the non-discrimination rules. They apply in case of the identifiable individuals but also to anonymous members of the group.[388]

Profiles or decisions based on certain criteria (health data, nationality, income, etc.) may lead to discrimination against individuals. It is difficult to determine when it is objectively justified to use such data and criteria, and when they are discriminatory (for instance, the processing of health-related data by insurance companies leading to decisions to raise premiums). Further legislative clarity would be desirable.

However, certain negative dimensions of profiling still escape from the regime of non-discrimination law (e.g., manipulation of individuals' behaviour by targeted advertising). Here no remedies have been identified.

The non-discrimination rules should be read in conjunction with the fairness principle of data protection law. The application of the two may have similar aims and effects; they might also be complementary (Can the limitations of non-discrimination law be justified if they are regarded as not fair, as in the example of the insurance companies raising premiums after processing health data?). They can address a range of actions undertaken in AmI, such as dynamic pricing or refusal to provide services (e.g., a refusal of service on the ground that no information (profile) is available could be regarded as discriminatory.).

Non-discrimination rules should be taken into consideration at the design stage of technology and service development.

Universal services

The universal service directive[389] provides for a minimum of telecommunication services for all at an affordable price as determined by each Member State. Prices for universal services may depart from those resulting from market conditions.[390] Such provisions aim at overcoming a digital divide and allowing all to enjoy a certain minimum of electronic services. The directive is definitely a good start in shaping the Information Society and the AmI environment. The development of new technologies and services generate costs, both on individual and the society at large. Many high-added-value AmI services will be designed for people who will be able to pay for them. Thus, AmI will reinforce the

[387] However, such issues might be addressed by the data protection legislation. In the opinion of Gutwirth & De Hert, principles of data protection are appropriate to cope with profiling. Hildebrandt, M. & S. Gutwirth (eds.), *Implications of profiling practices on democracy and rule of law*, FIDIS Deliverable D7.4, September 2005. http://www.fidis.net/fidis_del.html.

[388] Custers, B., *The Power of Knowledge, Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen, 2004, pp. 164-165.

[389] 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) *OJ L 108 , 24/04/2002 p. 0051 - 0077*

[390] More on the directive in Friedewald M., E. Vildjiounatie and D. Wright (eds.), *The brave new world of ambient intelligence: A state-of-the-art review,* SWAMI Deliverable D 1, July 2005, p. 176.

inequalities between the poor and rich. However, it has to be ensured that all are enabled to participate in the benefits of AmI, at least at a minimum level. *The Commission should consider whether new emerging AmI services should be provided to all. Some services (e.g., emergency services) could even be regarded as public and provided free of charge or as part of social security schemes.*

Technical assistance

The AmI environment will need to feature interoperability and compatibility in order to operate at the global level. That raises the issue of standardisation, which is a precondition for ensuring the interoperability of systems, networks and information. But the creation of standards as well as the development of the new technology and services complying with those standards has a cost. There is a danger that AmI will widen the gap between the developed and developing world. *Therefore, there is a need for Europe to consider the utility of providing assistance to societies who need it so that they too can comply with technological standards and thus benefit from AmI.*

4.4.10 Specific recommendations regarding interoperability and IPR

General

The SWAMI deliverables 1 and 2 already emphasised that AmI will cause major problems for current intellectual property protection, because AmI requires interoperability of devices, software, data and information, e.g., for crucial information systems such as health monitoring systems used by travelling seniors. There is also the growing need for creating means of intellectual property protection that will respect privacy and allow for anonymous content viewing. Intellectual property rights give exclusive rights over the databases consisting of personal data and profiles, while the data subjects do not have a property right over their own information collected. We discuss these issues below.

Protection of databases and profiling

The directive on the legal protection of databases[391] provides for a copyright protection of databases, if they constitute the author's own intellectual creation by virtue of his selection or arrangement of their content. The directive also foresees a *sui generis* protection, if there has been a qualitatively and/or quantitatively substantial investment in either the obtaining, verification or presentation of the content. *Sui generis* protection "prevents the extraction and/or the re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database". This implies that the database maker can obtain a *sui generis* protection of a database even when its content consists of personal data. Although the user does not have a property right over his personal data, the maker of a database can obtain an exclusive right over this type of data. Hence, a profile built on the personal data of a data subject might constitute somebody else's intellectual property.

Some legal experts have proposed that property rights over personal data be granted to the data subject, and that he be empowered to consciously distribute this information (see above). It is doubtful if that would actually create any advantage for the data subject. Such

[391] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal* L 077, 27/03/1996, pp. 0020 – 0028.

an approach does not solve the problem of creating and then using the profiles based on such distributed data. Profiles created by the data processor will still constitute his property.

The right to information about what knowledge has been derived from one's data could, to some extent, provide a safeguard against profiling. We recommend that further research be undertaken on how to reconcile this with the intellectual property rights.[392]

DRMs

The copyright directive[393] provides for the protection of DRMs used to manage the licence rights of works that are accessed after identification or authentication of a user.[394] But DRMs can violate privacy, because they can be used for processing of personal data and constructing (group) profiles, which might conflict with data protection law.

Less invasive ways of reconciling intellectual property rights with privacy should be considered.

This not only relates to technologies but also to an estimation of the factual economic position of the customer. For example, the general terms and conditions for subscribing to an interactive television service – often a service offered by just a few players – should not impose on customers a condition that personal data relating to their viewing behaviour can be processed and used for direct marketing or for transfer to "affiliated" third parties.

As the Article 29 Working Party advises, greater attention should be devoted to the use of PETs within DRM systems.[395] In particular, it advises that tools be used to preserve the anonymity of users and it recommends the limited use of unique identifiers. Use of unique identifiers allows profiling and tagging of a document linked to an individual, enabling tracking for copyright abuses. Such tagging should not be used, unless necessary for performance of the service or unless with the informed consent of individual. All relevant information required under data protection legislation should be provided to users, including categories of collected information, the purpose of collecting and information about the rights of the data subject.[396]

The directive on the legal protection of software[397] obliges Member States to provide appropriate remedies against a person committing any act of putting into circulation, or the possession for commercial purposes of any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program. *The software directive only protects against the putting into circulation of such devices and not against the act of*

---

[392] See above, right to information.
[393] 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, *Official Journal* L 167 , 22/06/2001, pp. 0010 - 0019
[394] See also above, Privacy Enhancing Technologies.
[395] Article 29 Data Protection Working Party, *Working document on data protection issues related to intellectual property rights* (WP 104), adopted on 18 January 2005.
http://ec.europa.eu/justice_home/fsj/privacy/
[396] Idem.
[397] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17/05/1991, pp. 0042-0046.

circumventing as such. It would be advisable to have a uniform solution in that respect. DRM can also violate consumer rights, by preventing the lawful enjoyment of the purchased product. The anti-circumvention provisions should be then coupled with better enforcement of consumer protection provisions regarding information disclosure to the consumer. [398] *The consumer should always be aware of any technological measures used to protect the content he wishes to purchase, and restrictions in use of such content as a consequence of technological protection (as well as he should be informed about technological consequences of DRMs for his devices, if any, e.g., installing the software on the computer of the client).*[399] *Product warnings and consumer notifications should always be in place, as well as raising general consumer awareness on the DRMs.*

Decompilation right

The directive on the legal protection of software allows the decompilation of computer programs in order to achieve the interoperability of independently created computer programs with other programs. However, such right is only granted for the lawful users of the software, which can, in fact, make this exception very narrow.

As interoperability is a precondition for AmI, AmI would have to lead to limitations on exclusive intellectual property rights. One could actually argue that programs should be developed so that they are interoperable with each other. That implies creating standards applicable in this field. Broader scope of the decompilation right would be desirable.

The EU's current battle with Microsoft shows that it is trying to strengthen the decompilation right with support of competition law reasoning. Time will show what the outcome of the battle will be.

Standards

The creation and use of the same technical standards and regulations worldwide would also facilitate the achievement of worldwide interoperability. The ICT industry (and the music industry) seems not always capable of agreeing upon standards.

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.

Achieving worldwide interoperability based on standards could also lead to a narrowing of the digital divide. *Assistance to the countries and societies that cannot afford to comply with standards developed by the rich and technologically advanced countries seems necessary.*

---

[398] See also OECD, *Report on Disclosure Issues Related to the Use of Copy Control and Digital Rights Management Technologies*, DSTI/CP(2005)15/FINAL, 2006. https://www.oecd.org/dataoecd/47/31/36546422.pdf. For comments on consumer needs re DRM, see also INDICARE Project, "Content Providers' Guide to Digital Rights Management: Any side effects in using DRM?". www.indicare.org.

[399] Those restrictions might, *inter alia*, prevent the user from making backups or private copies, downloading music to portable devices, playing music on certain devices, or constitute the geographical restrictions such as regional coding of DVDs.

The directive on technical standards and technical regulations in Information Society services[400] provides a framework for exchange and creation of standards and information procedures to prevent the creation of the different standards. Though it is a step in the right direction, the issue of standards and interoperability emphasises again the necessity of closer international co-operation.

It is worth recalling here the initiatives to create privacy standards and a single vocabulary for privacy preferences. Among these initiatives are those of the World Wide Web Consortium and the Platform for Privacy Preferences (P3P).[401]

A uniform way of expressing privacy preferences is important today and even moreso for an AmI future. In the opinion of the Article 29 Working Party, such a common vocabulary should reflect the high privacy standards of data protection, and not lower common standards.

The Article 29 Working Party recommends *inter alia*:
(a) technical platforms for privacy protection must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals and
(b) browsing software sold or distributed within the EU must be designed and configured to ensure that on-line agreements in contradiction with prevailing data protection laws are not possible. It also recommends default privacy settings that would ensure a high level of the privacy protection is implemented into browser technology.

4.4.11 Specific recommendations regarding international co-operation

General

One of the main conclusions of SWAMI consortium is an emphasis on the urgent need for international co-operation in the development and deployment of AmI networks. Clearly, AmI has a global dimension. It enables real-time communication between users wherever they are. It enables a gesture by an arm with an implanted chip to control the movements of a robot on the other side of the ocean.[402] The actions taken by an individual in one place can have cross-border and global implications. It can actually be difficult to determine where certain actions with cross-border dimensions actually take place (e.g. processing the data). Crimes and torts committed in one place can cause results miles and miles away. Fighting against attacks would largely be ineffective without international co-operation. Thus, international cooperation seems to be necessity, also in providing a coherent legal framework for all interested actors (the biggest limitation of the legal rules existing today is their restriction to certain countries or to EU only).

---

[400] 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.*

[401] Working Party on the Protection of Individuals with regard to the processing of Personal Data, Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), XV D/5032/98, WP 11, 6 June 1998, ttp://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp11_en.pdf

[402] Example of the Warwick, K., "Wiring in Humans", presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006. See Friedewald, M., & D. Wright (eds.), *Report on the Final Conference*, Brussels, 21-22 March 2006, SWAMI Deliverable D5, 2006. http://swami.jrc.es/pages/documents/Deliverable5-ReportonConference.pdf

Jurisdiction in criminal matters

Currently there is no international or European framework determining jurisdiction in the criminal matters, thus, national rules are applicable. The main characteristics of the legal provisions in this matter have already been extensively discussed in previous SWAMI deliverables; however, it seems useful to refer here to some of our earlier conclusions. The analysis of the connecting factors for forum selection (where a case is to be heard) shows that it is almost always possible for a judge to declare himself competent to hear a case. Certain guidelines have already been developed, both in the context of the Cybercrime Convention[403] as well as the 2005 EU Framework Decision on attacks against information systems[404] on how to resolve the issue of concurrent competences. According to the Cybercrime Convention, "The Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[405]

The 2005 EU Framework Decision on attacks against information systems states, "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 actions. A sequential account may be taken of the following factors: (1) the Member State shall be the one in which the offences have been committed according to paragraph 1(a) and paragraph 2; (2) the Member State shall be the one of which the perpetrator is a national; (3) the Member State shall be the one in which the perpetrator has been found."[406]

Legal experts and academics should follow any future developments in application of those rules that might indicate whether more straightforward rules are needed. The discussion on the recently published Green Paper on double jeopardy should also be closely followed.[407]

Private international law

In the *Journey of the seniors* scenario in SWAMI deliverable 2, we discussed an accident involving German tourists in Italy, while travelling with a tourist company established in a third country. The international dimension of the actions taken in AmI could actually lead to the conclusion that fitting AmI into a legal framework based on territorial concepts might cause some problems. Such territorial connecting factors are currently used in legal rules dealing with the choice of law and jurisdiction. Often seen as the result of legal technicalities, rules on the choice of law or jurisdiction can have practical consequences. They have an impact on enhancing or decreasing the factual inequality between the parties. Clear rules determining the law applicable between the parties are an important guarantee

[403] Council of Europe - Cybercrime Convention of 23 November 2001.
[404] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ L 069, 16/03/2005 p. 67- 71.*
[405] Article 22 paragraph 5 Cybercrime Convention.
[406] Article 10 paragraph 5 *2005 EU Framework Decision on attacks against information systems.*
[407] Green Paper on Conflicts of Jurisdiction and the Principle of *ne bis in idem* in Criminal Proceedings COM(2005) 696, December 2005, accesible at http://ec.europa.eu/comm/off/green/index_en.htm

of legal certainty. They allow one to know what rules (i.e., which law) will apply to particular activities beforehand, and thus to know which rules to obey. Private international law is an important element that can facilitate the adherence to legal requirements. Clear rules on the applicable law and choice of jurisdiction can facilitate court actions and create an incentive for private enforcement of laws by individuals who sustain damages.

Private international law issues are dealt at the European level by two legal acts, the Rome Convention on the law applicable to contractual obligations[408] and the Brussels Regulation on jurisdiction and enforcement of judgments[409].

Jurisdiction in civil matters

The Regulation on jurisdiction and enforcement of judgments in civil and commercial matters covers both contractual and non-contractual matters. In the absence of a jurisdictional agreement between the parties, forum selection (where a case is to be heard) is generally assessed on the grounds of the defendant's domicile.[410] The regulation is also applicable for determining jurisdiction by non-EU plaintiffs against EU defendants.[411] Alternative rules on jurisdiction apply in the case of a contract in which the plaintiff may select the forum. However, criteria used by the regulation in such cases (e.g., the place of performance of the contract or of delivery of goods, where services were provided or where a harmful event occurred or might occur) might be difficult to determine, so that multiple fora could be competent to decide the case. In the case of contracts, the key factor is the place of performance of the contract. In the case of a contract for delivery of goods or services, the place of the performance should be understood as where the goods are delivered or where the services are provided. The place of the performance of the contract for the on-line purchase of goods or services awaits clarification.[412] In tort cases, the place where a harmful event occurred or might occur determines the competent court, however, it can be understand or as the place where the harmful event occurs, or where the damage is suffered.[413] If the dispute arises out of the operation of a branch, agency or other establishment, the competent court is determined by the place in which the branch, agency or other establishment is situated.[414]

---

[408] 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*

[409] 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.*

[410] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *Official Journal* L 012 , 16/01/2001, pp. 0001-0023. This regulation supersedes the Brussels Convention of 1968 (Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters (consolidated text) *Official Journal* C 27, 26/01/1998, pp. 1-27), and applies to all Member States except Denmark, where the Brussels regulation still applies.

[411] Schaub, M., *European Legal Aspects of E-commerce*, Europa Law, Groningen, Netherlands, 2004, p. 147.

[412] Gillies, L., "European Union: Modified Rules of Jurisdiction for electronic Consumer Contracts", *Computer Law & Security Report*, Vol. 17 No. 6, 2001, pp. 395-398 and Gillies, L., "A Review of the New Jurisdiction Rules for Electronic Consumer Contracts within the European Union", Commentary, The Journal of Information, Law and Technology (JILT), 2001 (1).
http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/gillies/

[413] The Bier case, C 21/76, ECR 2183.

[414] Article 5 (5) of the Brussels regulation. The electronic offices or agents, web server, or the accessibility of the web are not likely to suffice to be understood as the establishment in the meaning of the Regulation. Schaub, M., "European Legal Aspects of E-commerce", Europa Law, Groningen, Netherlands, 2004, p. 147.

The Regulation also provides special rules for exclusive jurisdiction that depart from the general rule. Consumer contracts are an example of such rules.[415] The consumer[416] may bring a case in the court of the company domicile or in his own domicile. On the other hand, consumers may be sued only in a court of their own domicile.[417] Such rules aim to enhance the position of the consumer who is generally the weaker party in a contractual relationship. These rules apply to a wide range of consumer contracts[418] as far as the consumer's contractor pursues commercial or professional activities on the territory of the consumer's Member State, or directs his activities there *by any means*. Though terms such as *pursue, direct activity* and *by any means* are ambiguous, they should be understood rather broadly, encompassing means of electronic communication, including websites.[419] Thus, this provision should be satisfactory and workable in AmI.

Provisions on the jurisdiction for consumer contracts apply when both parties are domiciled in EU Member States. However, the jurisdiction may also be established if the dispute arises out of the operation of the branch, agency or other establishment of the defendant in the Member State.[420] Despite such provisions broadening the scope of application of the regulation, a substantial number of businesses offering services to EU consumers stay outside the reach of regulation.

---

[415] In fact, the Brussels regulation amended the provision on consumer contracts in order to adjust them to electronic commerce. On the process of developing new rules and the approval of the regulation, see Gillies L., "A Review of the New Jurisdiction Rules for Electronic Consumer Contracts within the European Union", *l.c.*

[416] Consumer contracts are regulated by Articles 15-17 of the Brussels Regulation.

[417] Article 16 of the Brussels Regulation.

[418] Article 15 (1) of the Brussels Regulation: These rules apply when (a) it is a contract for the sale of goods on instalment credit terms or (b) it is a contract for a loan repayable by instalments, or for any other form of credit, made to finance the sale of goods or (c) in all other cases where the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities in that Member State or several States including that Member State, and the contract falls within the scope of such activities. The most relevant is the last and the broadest category. This "catch-all" category in Article 15 (3) of the Brussels Regulation excludes the contracts of transport other than contracts that, for an inclusive price, provide for a combination of travel and accommodation. Thus, on-line ticket bookings are excluded, though holiday packages are not. See Schaub, Martien, "European Legal Aspects of E-commerce", Europa Law, Groningen, Netherlands, 2004, p. 153 and Gillies, L. "European Union: Modified Rules of Jurisdiction for electronic Consumer Contracts", *Computer Law & Security Report*, Vol. 17 No. 6, 2001, pp. 395-398.

[419] It is stated that contracting only with interactive websites will provide the basis for the application of the protective rules on jurisdiction. Providing the information on the service or goods (passive websites) does not result in such effect; see Explanatory Memorandum, COM (1999) 348 Final, Brussels 1999, p. 16. The term "direct activity toward one or more Member States" can also be broadly understood: the existence of a consumer contract might be understood as an indication of the supplier's directing his activities towards his Member State. See Amended proposal for a Council Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters; Schaub, Martien, "European Legal Aspects of E-commerce", Europa Law, Groningen, Netherlands, 2004, p. 154; Gilles, L., "European Union: Modified Rules of Jurisdiction for electronic Consumer Contracts", *Computer Law & Security Report*, Vol. 17 No. 6, 2001, pp. 395-398 and "A Review of the New Jurisdiction Rules for Electronic Consumer Contracts within the European Union", Commentary, 2001a, *The Journal of Information, Law and Technology (JILT)*. http://elj.warwick.ac.uk/jilt/01-1/gillies.html. Such distinctions and discussions are less relevant for AmI where the environment will actively interact with the consumer (or his intelligent agent), offering the goods and services specially targeted at him.

[420] Article 15 (2) of the Brussels Regulation. See the comments under 134. Although it is possible that, in the future, the localised webpage would be understood as the establishment in the understanding of this particular provision. Schaub, Martien, "European Legal Aspects of E-commerce", Europa Law, Groningen, Netherlands, 2004, p. 147.

In cases where the defendant is domiciled outside the EU, the regulation will not provide a solution for forum selection[421]*, nor do the provisions on the jurisdiction in consumer contracts. This emphasises again the limitation of the discussed solution to the territory of the Member States and the need for a more global approach.*[422]

Clarification and simplification of the forum selection for non-consumers would also be desirable. It seems that the complexity of the business environment, service/product creation and delivery would justify such approach. It would be of special importance for SMEs.

Applicable law

Currently, the applicable law for contractual obligations is determined by the 1980 Rome Convention.[423] Efforts have been undertaken to modernise the Rome Convention and replace it with a Community Instrument. Recently, the Commission has presented the proposal for a regulation of the European Parliament and the Council on the law applicable to contractual obligations.[424] A comparison of the relevant provisions of the Convention and the new proposal follows.

As we have identified in our previous deliverables[425], the biggest weakness of the Rome Convention seem to be its limitation to contractual issues only. Although contracts will be crucial for the AmI environment, it is more than desirable to provide a clear set of rules for non-contractual relationships. Some initiatives have already been undertaken in that direction.[426]

A feature of the Rome Convention is that it relies heavily on the territorial criterion. It refers to the habitual residence, the central administration or place of business as the key factors determining the national law most relevant to the case.[427] But IT services can be

[421] Article 4 of the Brussels Regulation states: 1. If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Articles 22 and 23, be determined by the law of that Member State; 2. As against such a defendant, any person domiciled in a Member State may, whatever his nationality, avail himself in that State of the rules of jurisdiction there in force, and in particular those specified in Annex I, in the same way as the nationals of that State.

[422] Ofcom, the UK regulator for communications, has made a similar point: "the global reach and open nature of the internet gives rise to some well-known problems, which cannot be addressed by a translation of existing powers and structures." *Online protection: A survey of consumer, industry and regulatory mechanisms and systems*, 21 June 2006, p. 1.
http://www.ofcom.org.uk/research/technology/onlineprotection/report.pdf

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

[424] The Commission has presented the proposal for a regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I), COM (2005) 650 final, 2005/0261 (COD).

[425] Friedewald M., E. Vildjiounatie and D. Wright (eds.), *The brave new world of ambient intelligence: A state-of-the-art review,* SWAMI Deliverable D 1, July 2005, p.172.

[426] We refer here to the Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations ("Rome II"), COM(2003) 427 final 2003/0168 (COD). http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0427en01.pdf

[427] According to Article 4, "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 unincorporated, its central administration. However, if the contract is entered into in the course of that party's trade or profession, that country shall be the country in which the principal place of business is situated or,

supplied at a distance by electronic means. The AmI service supplier could have his habitual residence or central administration anywhere in the world and he could choose his place of residence (central administration) according to how beneficial is the national law of a given country. The habitual residence factor has been kept and strengthened in the Commission's proposal for a new regulation replacing the Rome Convention (Rome I proposal, Article 4).[428]

The Rome Convention creates specific rules for consumer contracts. Those rules are built upon the notion of the *habitual residence* of the consumer. Such a criterion, generally more useful since it has the potential to provide greater protection of the consumer (as well as better clarity of the rules applicable to the parties. It is often easier to determine the *habitual residence* of the consumer than, e.g., *place of performance of the contract.*), is still not free of problems. In AmI, the notion of a habitual residence might be flexible and often difficult to apply. At the same time, however, application of the law with regard to the habitual residence of the consumer is rather the exception than the rule under the Convention. Article 5 restricts application of this consumer protection provision to contracts that have been entered into in specifically defined circumstances.[429] Despite the fact that the scope of some of these exceptions may actually be broad in AmI,[430] such construction can always lead to uncertainty and differences in interpretation when assessing a particular case. AmI will also bring specific problems in application of this rule. Since the provision requires the consumer to take all the steps necessary on his part for the conclusion of the contract in the country of his habitual residence, the consumer loses that protection when travelling and ordering goods from different destinations. This is regrettable, especially since AmI is built on mobility.[431] Moreover, Article 5 does not apply to a contract for carriage or to a contract for the supply of services to the consumer exclusively in a country other than the one of his habitual residence.[432] It does, however, apply to a contract that, for an inclusive price, provides a combination of travel and accommodation. Such a limitation may exclude an important number of AmI services from coverage by the Convention.

---

where under the terms of the contract the performance is to be effected through a place of business other than the principal place of business, the country in which that other place of business is situated."

[428] The new proposal does not use the presumption that the country of habitual residence is the most closely connected with the case, as it is under the Rome Convention. In the proposal, the relevant factor of the habitual residence of, *inter alia*, seller or service provider is the fixed rule.

[429] (Article 5 point 3 in conjunction with point 2) 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
- if the other party or his agent received the consumer's order in that country, or
- 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.

[430] We especially refer here to the situation where the conclusion of the contract in the country of the habitual residence of the consumer 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. However, there are different views on what the "specific invitation" means in relation to cyberspace. Some claim that a restrictive approach should be taken, and thus a website would constitute "specific invitation" only in those countries towards which it is specifically directed (by using the national domain name or language), thus there is the possibility of limiting the exposure of the company to the mandatory rules of consumer laws. Others say that the Internet is built on the concept of global accessibility, and therefore the company targets the consumer world-wide via the Web. For discussion, see Schaub M., *European Legal Aspects of E-commerce*, Europa Law, Groningen, Netherlands, 2004, p.164.

[431] Thus the usage of mobile devices is not fully addressed. See Schaub, M., *o.c*, p.164.

[432] Article 5 points 4 and 5 of Convention

The new proposal for the Rome I regulation amends the consumer protection provisions.[433] It still relies on the *habitual residence* of the consumer, but it brings the consumer contract choice of law in line with the equivalent provisions of the Brussels regulation. The *targeted activity* criterion (applicable under the Brussels regulation) has replaced the specific conditions of article 5 (2) of the Rome convention (circumstances under which the contract was entered into). The scope of these provisions has been broadened, since they apply not only to the contracts for the supply of goods or services (as under the convention), but also to all contacts, unless explicitly excluded. The requirement to take all necessary steps to conclude the contract in the country of the habitual residence has been abolished. On the other hand, the provision does not apply to the situation when the consumer contractor does not know where is the habitual residence of the latter and where this is not his fault.

The Rome Convention applies when parties to the legal relationship have not chosen applicable law. The service supplier may often impose the choice of law applicable to the contract (as well as the choice of jurisdiction). Some mandatory rules of the law of the habitual residence of the consumer could still apply in the case of consumer contracts. Also in this case, it is rather an exception than a general rule. It seems to aim at determining a closer connection with a particular territory (here the place of habitual residence of the consumer). Similarly, in the case of mandatory rules that shall apply in case of contracts in general, an important limitation comes into play. The Rome Convention stipulates that, "where all the other elements relevant to the situation at the time of the choice are connected with one country only", the choice of law by the parties cannot prejudice the application of rules of the law of that country (Article 3 (3) of the Rome Convention). As we will frequently encounter trans-border situations in AmI, however, the criterion of the "relevant elements of the case connected with one country only" makes this stipulation basically not applicable. Moreover, in AmI, the boundaries between places and spaces will be diminishing, and it will be difficult to connect some of the elements of the case with any particular territory. A similar provision can be found in the Commission proposal for Rome I (Article 3 (4)). However, the following paragraph of the proposal states that when the parties choose the law of a non-Member State, such choice is without prejudice to the mandatory rules of Community law, thus providing a minimum protection for individuals.

The Commission proposal for the regulation on the law applicable to contractual obligations is in any aspect a good step forward. It is to be seen if it becomes the binding law.

Some other legislative acts also contain rules on applicable law. Most important are provisions in the data protection directive. This directive also chooses the territorial criterion to determine the national law applicable to the processing of data, which is the law of the place where the processing is carried out in the context of the activities of an establishment of the data controller. Such a criterion, however, might be problematic: more than one national law might be applicable to the case.[434] Moreover, in times of

[433] As recital 10 of the proposal states, these amendments aim to take into account the developments in distance selling, thus including ICT developments.

[434] Article 4 (1) of the directive stipulates: Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures

globalisation of economic activity, it is easy for an undertaking to choose the place of establishment, which would guarantee him the most liberal regime, which might avoid the application of the European data protection law. In situations when a non-EU state is involved, the directive points out to the different relevant factor, the location of the equipment used[435], thus enabling broader application of the EU data protection directive.[436]

As we see, in all these cases, the territorial criterion (establishment) prevails. *We should consider moving towards a more personal criterion, especially since personal data are linked with an identity and a state of a data subject (issues which are regulated by the national law of the person). Such a criterion could be more easily reconciled with the AmI world without the physical borders of high mobility.* The data subject will also be able to remain under the protection of his/her national law, and the data controller/service provider will not have the possibility of selecting a place of establishment granting him the most liberal treatment of law... Such a solution is justified by the special characteristics of the AmI environment and would offer better clarity on how to deal with such situations. *The criterion of the habitual residence of the consumer will have such effect in many instances. The alternative solution would be to use the criterion of the location of the equipment used for the processing of data, as the one foreseen in the data protection directive.*[437]

Data transfer

Data transfer is another issue emphasising the need for international co-operation in the creation of a common playing field for AmI at the global level. What is the sense of protecting data in one country if they are transferred to a country not affording comparable (or any) safeguards? Also, the globalisation of economic and other activities brings the necessity of exchanging personal data between the countries. The data protection directive provides a set of rules on the data transfer to the third countries.[438] The data can be

---

to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

[435] The directive stipulates in article 4 (1) that the national law of a given Member State will apply when the controller is not established on Community territory and, 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.

[436] The Article 29 Data Protection Working Party interprets the term "equipment" as referring to all kinds of tools or devices, including personal computers, which can be used for many kinds of processing operations. The definition could be extended to all devices with a capacity to collect data, including sensors, implants and maybe RFIDs. (Active RFID chips can also *collect* information. They are expensive compared to passive RFID chips but are already part of the real world.) See Article 29 Data Protection Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites* (5035/01/EN/Final WP 56), 30 May 2002. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

[437] Such a solution has the advantage of covering, with the protection of EU legislation, third country residents whose data are processed via equipment in the EU. A broad interpretation of the term "equipment" would help guarantee the relatively broad application of such rule (see above). As a result, in most cases, application of the domicile/nationality rule or the place of the equipment used as the relevant factor would have the same result. However, we can envisage the processing of data not using such equipment, for example, when the data are already posted on-line. Then the EU law could not be applicable.

[438] On 30 May 2006, the European court of justice ruled that it was unlawful to order European airlines to hand over information about transatlantic air passengers to the US government. The court said the US did not provide adequate protection for air passengers' privacy. Under the Passenger Name Records agreement, reached in May 2004, EU airlines have been obliged to give Washington 34 items of information about passengers flying to the US. The court said the agreement had to be annulled because existing EU data protection law only covers commercial data and not that used for security purposes. See Sturcke, James and agencies, "US access to flight data unlawful", *The Guardian*, 30 May 2006.

transferred only to countries offering an adequate level of protection. The Commission can conclude agreements (e.g., the Safe Harbour Agreement) with third countries that ensure an adequate level of protection. The Commission can also issue a decision in that respect. However, the major problem is again enforcement of such rules, especially in view of the fact that some "safeguards" rely on self-regulatory systems whereby companies merely promise not to violate their declared privacy policies (as is the case with the Safe Harbour Agreement*). Attention by the media and consumer organisations can help in the enforcement of agreed rules. The problem of weak enforcement also emphasises the need to strengthen international co-operation with the aim of developing new enforcement mechanisms. Providing assistance in good practices in countries with less experience than the EU might also be very useful.*

5 CONCLUSIONS AND RECOMMENDATIONS FOR STAKEHOLDERS

In Chapter 4, the SWAMI partners have identified safeguards against the threats and vulnerabilities affecting privacy, identity, trust, security and the digital divide in an AmI world. We commend implementation of these safeguards. In this chapter, we offer some specific recommendations addressed to particular stakeholders some of which flow from the safeguards identified above.

5.1 ADOPTING A RISK ASSESSMENT – RISK MANAGEMENT APPROACH TO AMI

Since their creation, the Internet and the World Wide Web[439] have become a critical infrastructure, arguably *the* critical infrastructure in virtually all countries and all societies. The Internet's interconnectedness and the dependency of other critical infrastructures (banking, transport, telecoms, electricity, water, etc.) upon it have made it indispensable to the functioning of our societies and economies. Further, many people now use the Internet more every day than they watch TV. As exponential as has been its growth and as pervasive as it has become, the Internet is just a stepping stone on the way to an even more pervasive network and set of technologies that will provide us with ambient intelligence.

Yet the development and implementation of ambient intelligence is taking place with little involvement of the wide range of stakeholders in an assessment of the risks (especially to security) that it poses. And, it's important to recall, risks are not static. Risks are growing as things become more interconnected.[440] No one has yet called for the rigour of a formalised risk assessment / risk management process for deployment of AmI even though it will have far-ranging impacts on our way of life. AmI offers great benefits, but poses great risks too.

Of course, no such process was followed when the Internet was constructed, but that is no reason to forsake such a process for AmI. Also, most people in the early 1990s were unaware of the coming of the Internet and the WWW, nor of how quickly they would take root. Such is not the case with AmI. Many people know AmI is coming and many experts have already starting raising yellow flags of caution: despite its many benefits, AmI will not be risk free.

Some people undoubtedly, and perhaps even justifiably, might argue that the development of ambient intelligence per se does not require a formalised risk assessment / risk

[439] See Wikipedia on the Internet: "The first TCP/IP wide area network was operational by 1 January 1983, when the United States' National Science Foundation (NSF) constructed a university network backbone that would later become the NSFNet. (This date is held by some to be technically that of the birth of the Internet.) It was then followed by the opening of the network to commercial interests in 1995… In August 1991 CERN publicized the new World Wide Web project, two years after Tim Berners-Lee had begun creating HTML, HTTP and the first few web pages at CERN. In 1993 the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign released the Mosaic web browser version 1.0, and by late 1994 there was growing public interest in the previously academic/technical Internet. By 1996 the word "Internet" was common public currency, but it referred almost entirely to the World Wide Web."

[440] "As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities." OECD *Guidelines for the Security of Information Systems and Networks: Towards a culture of security*, OECD, Paris, 2002, p. 7. The OECD has made the point in other of its reports too. See, for example, *Emerging Risks in the 21st Century*, 2003, p. 13: "The openness and connectedness of systems and … technology and information increase the number of potential interactions that can generate or influence a hazard. Risks become more complex."

management process. But, if anything, SWAMI hopes and trusts it has demonstrated from its reports that ambient intelligence, as wonderful as it may seem, is not risk free, that it poses serious risks, not only to our privacy (and, as a consequence, to our democratic values), but also to our security.

Our privacy is already being eroded relentlessly, day by day. In a world of ambient intelligence, it will be extremely difficult to protect what privacy we have left. The pervasiveness of AmI, one of its most touted features, is a double-edged sword. While it offers great benefits, it also poses great threats, especially to our privacy. The vast amount of data that will be generated in an AmI world will be virtually impossible to contain and control. Which is not to say that efforts shouldn't be made, that we should simply throw up our hands in despair. On the contrary, efforts *must* be made to ensure that this deluge of data is not abused.

To some, especially those in positions of power, privacy may seem like a disposable value, soft, intangible, difficult to quantify in terms of its value. We and many others have, however, argued that privacy is a cornerstone value of our democracy, that as it erodes, we must be increasingly vigilant about the threats such erosion poses to our democracy. Ambient intelligence enables constant surveillance, not just of the Orwellian video variety, but also of a much more intimate variety. Ambient intelligence enables surveillance of what we are doing and where we are at all times. Intelligent software, a key feature of the personalisation of AmI services, will allow people with corporate and political power, to predict what we will want, how we will behave. Networked sensors that can monitor our physiological well-being, while of obvious medical benefit, also pose a risk that they can monitor our reaction to various stimuli.

The walls of our homes and the skins of our bodies will no longer be a shield against prying eyes. The sanctity of our homes and of our thoughts and behaviour is disappearing.[441] AmI will make it possible to monitor what we do, how and what we are (supposedly) thinking, wherever we are, whether on the street, in a shop, in our homes and virtually in our minds.

Despite the unreliability of today's profiling and the huge number of false positives, profiling will continue, because there are strong commercial and political incentives to do so. Profiling is necessary for the personalisation of services. It is also regarded as necessary for crime prevention and pre-empting acts of terrorism. The proponents of profiling may admit that it's an imperfect science, but it will get better. The more information there is, the more precise profiles can be.

The relentless surveillance, massive data mining and analysis, and profiling enhance and erode our security at the same time. The rapid identification of the terrorists in the London bombings of July 2005 showed how beneficial surveillance could be. Constant, pervasive

[441] According to a Reuters report, "An 'emotionally aware' computer being developed by British and American scientists will be able to read an individual's thoughts by analysing a combination of facial movements that represent underlying feelings. 'The system we have developed allows a wide range of mental states to be identified just by pointing a video camera at someone,' said Professor Peter Robinson, of the University of Cambridge in England. He and his collaborators believe the mind-reading computer's applications could range from improving people's driving skills to helping companies tailor advertising to people's moods." Reaney, Patricia, "Coming soon: Mind-reading computers", Reuters, 26 June 2006. http://today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006-06-25T232536Z_01_L23596655_RTRUKOC_0_US-SCIENCE-COMPUTERS.xml&archived=False

surveillance and increasing the accuracy of profiling are expected (and rightly so too) to facilitate the prevention and pre-emption of criminal and terrorist activity. Minority Report is not an idle fantasy. Replace Spielberg's "pre-cogs" with ambient intelligence and we can see what's coming without the need for genetically engineered "pre-visions".

Orwell's *1984* was not an idle fantasy either. The omni-present surveillance depicted there has a chilling effect on democracy. Conformity is expected, deviant behaviour is not tolerated.

The development and deployment of ambient intelligence will not generate many *new* threats or vulnerabilities. Certainly, the threats and vulnerabilities that we know today will continue to be present in an AmI world. AmI will undoubtedly offer new ways to Big Brother (the state) and little brothers (big business) to watch us (surveillance) and our privacy will certainly be at greater risk than ever before, but while the technologies will offer new opportunities for surveillance and invasion of privacy, surveillance and privacy invasion, per se, exist today (as they have for thousands of years), so they cannot be regarded as *new* threats or vulnerabilities. Similarly, the threats to trust and our sense of identity that exist today will continue to be threats for the future. Inclusion will continue to be a challenge, and the digital divide most likely will endure. Even if there are few new classes of threats or vulnerabilities in AmI, one should not under-estimate their significance. What is especially new or different about an AmI world compared to today's world (or, even better, compared to the pre-Internet world) is the *scale* of data generated, the omnipresence and pervasiveness of the new technologies and, consequently, the scale of the risks that arise from (theoretically) connecting everything and everybody.

Opinion polls seem to suggest that some people are not so concerned about some of these risks. Many are willing to trade their privacy for greater security. People are willing to have the video cameras in the streets, shops, the Underground, airports, etc., because they think it will improve their security. There even seems to be substantial support for monitoring telecommunications and Internet usage, for eavesdropping and reading our e-mails.

People are less content, however, about the frequency of identity theft and spamming. Most people don't like encountering viruses and other malware or having their services disrupted by attackers. AmI won't stop these criminal activities. If anything, AmI will create new opportunities.

Given the magnitude of risks, not just to privacy, but also to security, it seems eminently reasonable (at least to the SWAMI partners) that a formalised risk assessment / risk management process should be initiated to consider the risks posed by AmI and the optimum way of treating them. Risk can never be eliminated, but some ways of treating risks are better than others. The key is involving stakeholders in the process in order to determine what ways of treating risks are the most socially acceptable, that have the most consensus of stakeholders.

We think all stakeholders should have the opportunity to participate in the process of assessing and managing the risks posed by AmI.

We are not alone in thinking so. In its guidelines towards a culture of security, the OECD has emphasised that "all participants are responsible for the security of information

systems and networks" and that "participants should conduct risk assessments". Further, it has been said that "security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats".[442]

We would not expect the outcome of any risk assessment – risk management process to call a halt to the deployment of AmI. Even if that were desirable, it is not practicable, nor feasible. In any event, deployment of AmI technologies has already begun.

We recommend that the Commission should initiate a consultation process. It should prepare an initial consultation document on AmI, outlining its benefits, threats and vulnerabilities, identify stakeholder groups and solicit their views with regard to those threats and vulnerabilities and the best ways of managing the risks, i.e., the ways that enjoy the widest support of stakeholders.

We think that a formalised risk assessment – risk management process would, if nothing else, help to raise awareness of AmI and the risks it poses. Consulting concerned citizens and those who represent citizens (including legislators) at the stage of development would increase the legitimacy of new technologies, how they should be deployed and used.

The Commission has invited the private sector to "Involve the insurance sector in developing appropriate risk management tools and methods to tackle ICT-related risks and foster a culture of risk management in organisations and business (in particular in SMEs)"[443]. SWAMI agrees with and supports this encouragement from the Commission, particularly, because "risk management tools and methods" have not much of a history in being applied to high tech social and security risks such as ambient intelligence. A Commission staff paper has also suggested that one option to improve the security of communication networks is to implement and maintain adequate risk management systems based on recognized international standards.[444] However, while it is good that the Commission recognises the value of applying risk management tools and methods to ICT-related risks, we do not think that this Commission goes far enough, particularly in involving all stakeholders, as we recommend. Furthermore, the aforementioned option would involve EU legislation imposing detailed technical and organisational obligations for providers of electronic communications networks and/or services, whereas SWAMI recommends that the Commission initiate the risk management process described above. We agree with the Commission when it says, "Identifying and meeting security challenges in relation to information systems and networks in the EU requires the full commitment of all stakeholders" [445], but getting that commitment, there's the rub. In order to get that

[442] OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security, OECD, Paris, 2002, pp. 10-12.

[443] European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006], p. 9 (section 3.3.2). http://ec.europa.eu/information_society/doc/com2006251.pdf

[444] Impact Assessment: Commission Staff Working Document, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the EU Regulatory Framework for electronic communications networks and services, SEC(2006) 817, Brussels, 28 June 2006, p. 27.
http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/public_consult/review/impactassessment_final.pdf.

[445] Ibid, p. 9 (section 4).

commitment, stakeholders must be given and encouraged to play a meaningful role from the outset of the risk management process, rather than simply leaving it up to the private sector and the insurance industry to devise some appropriate tools.

5.2 RECOMMENDATIONS FOR THE EUROPEAN COMMISSION

5.2.1 Research and development

The development of AmI safeguards should be supported as much as possible, especially because they are the main means expected to help protect people from accidental, unintentional privacy violation.

Further harmonisation of standards with varying degrees of geographical scope will be needed (e.g., EU, international). Some countries, however, will not be able to afford to fully comply with the standards created in developed countries. Solutions to overcome the potential divides based on insufficient interoperability need to be envisaged.

The Commission should ensure that privacy, identity, trust, security and digital divide issues are taken into account in any project it supports. As has been demonstrated, it is crucial to integrate privacy and security aspects from the very beginning in any development process. Once certain technical platforms, standards or system designs are established, it is often too late or associated with unreasonably high additional costs to adequately include appropriate safeguards.

Research on technologies that could help protect our privacy and strengthen the security of networks and devices (against attackers and other vulnerabilities), and that could help to minimise the digital divide should be increased (see section on technical safeguards). Certain problems cannot be solved by other than technology means: if there are no human-technology interfaces for all categories of possible users (including disabled users or people capable of speaking only one language), then the digital divide will continue to exist. If no user-friendly security exists (and current authentication procedures are not really user-friendly), security recommendations will not be followed. Consequently, research on critical technological safeguards is very important.

Hence concrete, step-by-step initiatives such as the EC-initiated consultation on RFIDs in March 2006[446] are to be welcomed. Further research on the RFID technology and its privacy implications is recommended. This research should also aim at determining whether any legislative action is needed to address the specific privacy concerns of RFID technology. We also recommend further development of codes of conducts and good practices with regard to the use of RFIDs. The EC consultation on RFIDs may address this recommendation.

Similar consolations with regard to other relevant technologies and concepts, e.g., biometrics and interoperability, could be considered. The implications for privacy caused by other technologies, such as location-tracking systems, physiological sensors, video and audio sensors should be evaluated, and good practices in use of these technologies should be developed and widely promulgated.

[446] http://www.rfidconsultation.eu/

5.2.2 Internal market and consumer protection

Prevent discriminatory service refusal

Effective safeguards to reduce the possibility of ill-founded service refusals mainly apply to the regulatory sphere.

- Regulations and user-friendly tools (which present all relevant information in concise and impressive form, perhaps with examples of possible negative consequences) need to provide for sufficient transparency. This would contribute to strengthening the customers' position and serve as a limitation to the exploitation of asymmetric power relations.
- AmI applications should be implemented preferably on the basis of an opt-in option (the user explicitly chooses to accept the application). In cases when applications are built in such a way that they are constantly attentive to all people around (e.g., to all visitors of a smart space), an option to opt-out needs to be incorporated, confining disadvantages as far as possible.
- Alternative procedures need to be available at reasonable cost in case of technical failures or if individuals request access without having the ability to meet the technical standards.
- Users should have the option to switch off different functionalities of personal devices independently of each other, unlike the current situation when many types (although not all) of mobile phones keep wireless connection always on when the phone is switched on, so that it is impossible to use, for example, the calendar application without your service provider's being aware of your current location.

By the same token, individuals should have the option to switch off their personal AmI devices (either completely or selected functionalities, e.g., to switch off wireless communication) so that even if they are being captured by surveillance cameras, their own devices are not contributing to their being tracked. Effective, free, informed and specific consent should be the basis of the EU policy regarding the internal market and consumer protection.

Prevent victimisation

As in the case of service refusals, in order to reduce the adverse side-effects of victimisation based, for instance, on faulty profiling, secondary back-up procedures need to be in place, incorporating additional contextual information which enable authorities to take informed decisions without being entirely dependent upon a technical system.

Electronic commerce and consumer protection

The e-commerce directive should be updated to include the possibility of concluding contracts by electronic means (including reference to intelligent agents). In any updating of the directive, there is also a need to facilitate the usage of pseudonyms, trusted third parties and credentials in electronic commerce. Intelligent agents could also assist consumers in the management of (electronic) information to which, under the law, they are entitled.

An increasing number of service providers will be involved in AmI services and it may not be feasible for all of them to provide the required information about their data processing

activities to consumers. One solution may be a requirement to provide such information about only the service provider whom the consumer directly pays and who is responsible to the consumer (joint liability would apply).

In an AmI world, services will be provided instantly and will be increasingly personalised. In many cases, the right of the consumer to withdraw from the service may not be applicable, feasible or practicable. New solutions should be developed to address this problem.

5.2.3 Privacy and security policy framework

On 31 May 2006, the Commission issued a communication in which it proposed a strategy for a secure Information Society.[447] SWAMI agrees with and supports the measures set out in the communication, however, as mentioned elsewhere in this document, we do not think that it goes far enough. The strategy proposes measures that the Commission itself, Member States, the private sector and individuals can take to combat the bad guys who are responsible for attacking our network and information security. There is an implicit assumption that the bad guys who are "increasingly motivated by profit rather than by the desire to create disruption for its own sake" are someone else. However, we are reminded of the famous line from Pogo, the cartoon strip from the 1960s: "We have met the enemy and he is us."[448] We have, we trust, cited a sufficient number of press reports in the course of the various SWAMI reports to indicate that the bad guys are not just rogue individuals from rogue states, but also governments and the private sector here at home.

The Commission "proposes a dynamic and integrated approach that involves allstakeholders", but is rather thin on specific initiatives with regard to involving users and civil society organisations. It mentions a "structured multi-stakeholder debate" and cites the planned Conference "i2010 – Towards a Ubiquitous European Information Society" being organised by the forthcoming Finnish Presidency, as a contribution to this debate. It also proposes "a seminar reflecting on ways to raise security awareness and strengthen the trust of end-users in the use of electronic networks and information systems". However, given the seriousness and pervasiveness of the risks to security and privacy posed by AmI, we think such initiatives are a good start, but do not go far enough.

Security should be valued as a collective asset. It is a collective good that should in principle be open for everyone. Governments should not leave choices regarding security open to the individual or to the market alone, but impose high standards and invest necessary means. To claim security rights with such a strong collective basis, associations of all kinds are far better placed than individuals. If privacy and security have a future, associations should be allowed to defend them in court.

---

[447] European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006]. http://ec.europa.eu/information_society/doc/com2006251.pdf

[448] Walt Kelly, Pogo's creator, first used the line "We Have Met The Enemy and He Is Us" on a poster for Earth Day in 1970. In 1972, it was the title of a book, *Pogo: We Have Met the Enemy and He Is Us*.

5.2.4 Correcting the lacunae that exist in legislation, regulation

The SWAMI consortium recommends that most of the challenges of new AmI environments be met by legal instruments that do not prohibit new technologies but channel them (transparency tools). In practice, this means data protection and security measures, rather than criminal law prohibitions and heavy administrative burdens. Transparency should be the default position, although some prohibitions referring to the political balances, ethical reasons, or core legal concepts should be also considered in policy discussion.

The SWAMI consortium recommends respect for the diversity and plurality of law-makers within Europe. Without under-estimating the role of the EU institutions, it would not be beneficial to single out these institutions as the sole responsible institutions and lawmakers for the AmI environment. The proposals produced by different stakeholders should be taken into consideration and they should be actively involved in policy discussions. Development of case law should also be closely observed.

In initiatives leading to standardisation of technical specifications for RFIDs, as well as any other similar technology, data protection concerns should be reflected. Privacy assessment of each particular RFID application could be a legally binding obligation

Development of a participatory impact assessment procedure would allow stakeholders to quickly identify and react to any negative features of technology.

A legal framework for sharing knowledge from AmI-generated profiles should be developed, as well as legal protection of technical solution enabling such information management. A legal framework is needed to cover automated protocols for policy negotiations as well as automated schemes imply that the consent of the data subject. The legal framework should cover situations wherein the explicit consent of the data subject for each collection of data is replaced by a “consent” given by an intelligent agent.

It is necessary to consider development of legal rules (and observe their development) with regard to issues that are specific to AmI. In that respect, we propose legal schemes be developed for digital territories as an important safeguard of privacy in the digital world of AmI. Especially, we propose to protect such territories against unlawful and unnecessary interference. The specific legal schemes would also be necessary to address the use of software agents and PETs.

The consumer should always be aware of any technological measures embedded in any product he purchases, and restrictions in use of such product as a consequence of technological protection. This applies to technology used to protect the content he wishes to purchase (and the consumer should be informed about technological consequences of DRM installed on his devices), and RFID applications. Product warnings and consumer notifications should always be in place, and should serve to raise consumer awareness about the DRM, RFID and any other technologies having similar impacts.

The right to information (manageable by intelligent agents) is not only a safeguard of consumer rights, but also a privacy safeguard. Thus, we think the individual should have access to information, in both human and machine-readable form, possibly facilitated by use of user-friendly information notices.

Effective liability rules, facilitating proof and empowering individuals (via e.g. representative actions, reversing the burden of poof, strict liability rules), can have a big impact in enforcement of legal provisions. Further examination of such issues is merited.

With regard to the jurisdiction and applicable law, better clarity and legal certainty would be desirable. The Commission should consider a departure from the territorial criterion currently used in private international law towards a personal criterion based on the habitual residence of the consumer, especially since personal data are linked with an identity and a state of a data subject (issues which are regulated by the national law of the person).

The biggest weakness in enforcement of rights is the limitation of any European rules to Member States only, or to countries that have signed international conventions (Cyber crime convention). Clearly, IT and AmI have global dimensions. International co-operation in developing and enforcing the legal framework is necessary. Therefore, the development of a more comprehensive international co-operation framework that would take AmI technologies and capabilities into account is quite urgent.[449]

5.2.5 Socio-economic measures

The Commission should consider whether new emerging AmI services should be provided to all in the context of an updated universal services directive. Some services (e.g., emergency services) could be provided free of charge or as part of social security schemes.

5.3 Recommendations for the Member States

In the procurement of ICT products, emphasis should be given to critical issues such as security and trustworthiness.

Member States should consider introducing legislative prohibitions on the admissibility (or general acceptance of the exclusionary rule) of evidence obtained through privacy and/or data protection law infringements.

Appropriate authorities (e.g., the Data Protection Officer) should control and authorise applications of implants after the assessment of the particular circumstances in each case. When an implant enables tracking of people, people should have the possibility to disconnect the implant at any given moment and they should have the possibility to be informed when a (distant) communication (e.g., through RFID) is taking place.

[449] Ofcom, the UK communications regulator, echoes our conclusion with regard to today's Internet: "Effective consumer protection on the internet requires more significant levels of international cooperation than currently exist." Ofcom, *Online protection: A survey of consumer, industry and regulatory mechanisms and systems*, Office of Communications, London, 21 June 2006, p. 4.
http://www.ofcom.org.uk/research/technology/onlineprotection/report.pdf

We agree with the European Group on Ethics in Science and New Technologies that irreversible ICT implants should not be used, except for medical purposes. Further research on the long-term impact of ICT implants is also recommended.[450]

In addition to and in line with the right to remain anonymous goes the use of anonymous and pseudonymous credentials, accompanied by unlinkability in certain situations (e.g., e-commerce). Some reconciliation may be necessary between privacy requirements and accountability requirements, for example, in e-commerce. In fact, such mechanisms should always be foreseen when disclosing someone's identity or when linking information is not necessary. Such necessity should not be easily assumed, and in every circumstance more privacy-friendly technological solutions should be sought.[451] However, the use of anonymity should be well balanced. To avoid its misuse, digital anonymity could be further legally regulated, especially stating when it is not appropriate.[452]

Governments that have not yet done so should ratify the Cybercrime Convention. A "revision" mechanism would desirable so that signatories could negotiate and include in the convention definitions of new, emerging cybercrimes. Specific provisions criminalising identity theft and (some forms of) unsolicited communication could be included within the scope of the convention.

A means to prevent data laundering could be an obligation imposed on those who buy or otherwise acquire databases, profiles and vast amounts of personal data, to check diligently the legal origin of the data. If the buyer does not check the origin and/or the legality of the databases and profiles, he could be considered equal to a receiver of stolen goods and thus held liable for illegal data processing. An obligation could also be created which would require buyers to notify the national data protection officers when personal data(bases) are acquired. Persons or companies involved or assisting in data laundering could be made subject to criminal sanctions.

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.

Improving awareness and education should be the responsibility of Member States and/or regional or local authorities (following the subsidiarity principle).

5.4 RECOMMENDATIONS FOR INDUSTRY

An approach to alleviate concerns about latent operations and data misuse, thus reducing distrust, is to enhance transparency by effectively informing users about system procedures, purposes and responsibilities. Any networked device, particularly those used

[450] European Group on Ethics in Science and New Technologies, "Ethical Aspects of ICT Implants in the Human Body", Opinion to the Commission, 16 March 2005.
http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf

[451] Leenes, Ronald. Koops, Bert-Jan., "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No 3, 2005, p.37

[452] Compare Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society), Deliverable D3.2, July 2005, p. 35-36,. http://www.fidis.net

by consumer-citizens should come with a privacy warning much like the warnings on tobacco products.

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

The International Organization for Standardization (ISO) has developed helpful standards and evaluation criteria relevant for IT privacy and security including, most notably, the ISO 15408 and ISO 17799 standards.

Industrial organisations and leaders should highlight the value of ISO certification processes and established codes of practice.

Organisations that compile databases with personal data (even if such compilation is incidental to their primary lines of business) should state on their websites and on product information to what extent they are compliant with ISO 17799 and/or how they have implemented the standard. An organisation could also mention to what extent they follow other guidelines dealing with privacy and security, such as those produced by the OECD.

Those designing AmI networks should ensure that the networks have features that enable effective audits.

Industry should expend less effort on fighting new regulations and more effort on involving stakeholders in the assessment and management of risks to privacy, identity, trust, security and inclusiveness. Involving stakeholders at an early stage will minimise downstream risks.

With respect to use of key technologies of Ambient Intelligence (such as networking of devices and objects, location tracking, authentication etc), manufacturers, suppliers and network operators must do their utmost to avoid negative impacts of new technologies and the bad publicity that follows as a consequence. This will best be done by involving privacy advocates and public interest groups at an early stage in the development of new technologies, especially in actively seeking their views about possible impacts and how such impacts are best addressed.

Engineers and others should not regard technology as "neutral". New technologies often raise policy issues, and this is certainly true of ambient intelligence. AmI offers great benefits, but the risk of not adequately addressing public concerns could mean delays in implementing the technologies, a lack of public support for taxpayer-funded research and vociferous protests by privacy protection advocates.

As interoperability is a precondition for AmI, programs should be developed so that they are interoperable with each other. That implies a need for new standards applicable to AmI. However, AmI may lead to limitations on exclusive intellectual property rights. Broader scope of the decompilation right would be desirable.

Achieving worldwide interoperability based on standards could also lead to a narrowing of the digital divide. Assistance to the countries and societies that cannot afford to comply

with standards developed by the rich and technologically advanced countries is desirable and may be necessary.

5.5 RECOMMENDATIONS FOR CIVIL SOCIETY ORGANISATIONS

An alternative to peer-rating systems are credibility-rating systems based on the assessment of trusted and independent institutions, such as library associations, consumer groups or other professional associations with widely acknowledged expertise within their respective domains. Ratings should be based on systematic assessments against clearly defined quality standards.

Consumer associations and other civil society organisations (CSOs) could play a useful role as a mediator between service providers and individual consumers and, more particularly, in forcing the development of service contracts (whether real or implicit) between the service provider and the individual consumer. Consumer organisations could leverage their negotiating position through the use of the media or other means of communication with their members. CSOs could position themselves closer to the industry vanguard as represented in platforms such as ARTEMIS by becoming members of such platforms themselves. Within these platforms, CSOs could encourage industry to develop "best practices" in terms of provision of services to consumers.

5.6 RECOMMENDATIONS FOR ACADEMIA

Institutes of higher education should ensure that courses in ICT-relevant disciplines cover the following content:

- impacts of ICT on society,
- knowledge from technology assessment or from "impact and design research", which has come into being in the field of computing,
- promotion of awareness of development potential for health and the environment in the development phase of new technologies.

This content should, where possible, be integrated into existing school subjects, step by step. The focus should be on longer-term principles, and shorter-lived phenomena should be included only where they provide a clear example of a general principle. This measure requires several individual measures, including the incorporation of these issues into revised curricula and the further training of teaching staff.

Consumers need to be educated about the privacy ramifications arising from virtually any transaction in which they are engaged. An education campaign should be targeted at different segments of the population. Targeting school-age children should be included in any such campaign.

Universities should (continue to) participate in the development of technological safeguards, such as privacy and security protection in networks (including mobile, ad-hoc and sensor networks, as well as personal area networks), in personal devices and in smart spaces, in identity management systems and in developing technological means to minimise the digital divide (such as user interfaces for all, language translation tools, e-learning methods).

5.7 RECOMMENDATIONS FOR INDIVIDUALS

Users cannot be innocent bystanders and expect others to look after their interests with regard to privacy and security aspects of the emerging AmI world. We concur with the OECD when it says "Participants [including individual users] should be aware of the need for security of information systems and networks and what they can do to enhance security… Participants should be aware of the … good practices that they can implement to enhance security, and the needs of other participants."[453] At the same time, we recognise that such good advice will not (cannot) be taken onboard by all users, children and the elderly being the most obvious example.

5.8 USER CONTROL AND ENFORCEABILITY OF POLICY IN AN ACCESSIBLE MANNER

Throughout the SWAMI project, the partners have faced two problems. One is the trade-off between privacy and security. The comment has been made that an increase in security doesn't necessarily mean a further encroachment on privacy – indeed, security is necessary to protect personal data and our privacy: Networks must be secure, our personal devices, reliable, dependable and trust-worthy. But security is a multi-faceted term, with many dimensions. Our concern in the context of our first problem is where AmI technology is used to help protect society against criminals, terrorists and other miscreants who seek to exploit our personal data in questionable or wrongful ways.

In this latter sense, we are of the view that in an ambient intelligence world, an increase in security most likely *will* encroach upon our privacy. Surveillance cameras will continue to proliferate. We can assume that, whatever the law is, whatever privacy protections government and business *say* they honour, our telecommunications, e-mails and Internet usage will be monitored to increasing degrees. The same will be true of our interfaces with the world of ambient intelligence. The products we buy and use will be linked to us. Personal data will be mined, linked and processed, traded, shared and sold. Many such practices will be unjustified and will violate our rights and civil liberties. We assume or should assume that those encroaching upon our rights and civil liberties will be not only criminals, but (supposedly) legitimate businesses and governments. Even so, the majority of the population may be willing to accept such encroachments because they are genuinely concerned about their own security, that of their family and fellow citizens. The so-called war on terror has undoubtedly provided fertile ground for acceptance.[454] And when surveillance technologies lead to the capture of terrorists and arrest of criminals, many people will even say they are fortunate that they live in a society embedded with intelligence (or at least surveillance capabilities) that has made it possible to apprehend terrorists and criminals quickly.

[453] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD, Paris, 2002, p. 10.

[454] "Since the 2001 terror attacks, a slim majority of the American public has favored protecting security over preserving civil liberties, according to opinion pollsters." Mohammed, Arshad, and Sara Kehaulani Goo, "Government Increasingly Turning to Data Mining", The Washington Post, 15 June 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html

In an AmI world, we can expect to see a direct trade-off between privacy and security, where the latter refers to the safety of the individual and/or especially the community or society in which he or she lives. And we can assume that gains in security will be made at the expense of losses in privacy.[455] We do not see an easy solution to this problem: indeed, there may not be any. Perhaps the most we can hope for is that unjustified encroachments, abuses and violations will come to light and that offenders will be prosecuted. Coupled with this unhappy prospect is the need for users to be aware, to be vigilant at all times when and where their privacy is put at risk or might be at risk and what users can do, individually and collectively, to minimise those risks. We trust that the safeguards we have suggested in this report can go some distance towards minimising those risks.

The second problem lies in the trade-off between restricting the availability of personal data and personalisation of services. Many of the benefits of AmI lie in the availability of such data in order to personalise services. The greater the restrictions on such data, the greater is the risk that we will not enjoy the full benefits offered by AmI.[456] The restrictions on such data may be imposed by law or by the individual or even by model corporate citizens. Government and, especially, corporate service providers will inevitably want as much personal data as they can get in order to personalise services as much as possible. However, the law may set some limits on how much they can get and users with their personal devices and privacy-enhancing technologies may also set some limits. Where these limits are set partly depends on how much confidence or trust we (individually and collectively) may have in AmI networks (or any network for that matter). If we were confident in the security (in the first sense of the term mentioned above) of the networks and our devices and the software that drives them, then we might be willing to extend those limits and accordingly enjoy greater benefits from AmI. But breaches in networks and software are a daily occurrence today and as networks become increasingly interconnected and complex, we can (should) assume that breaches will continue to plague us for the foreseeable future. Theoretically, it might be possible to solve or at least greater reduce the risk of breaches in security, but then we run up against the human dimension of our first conundrum. Even if it is possible to build totally secure networks and services, how much trust are we willing to extend to governments and businesses or anyone that they will respect our privacy and not abuse it? Unfortunately, even if technology could be made reliable and secure, the prospect of changing human behaviour is even less promising.

Given the problems, the best prospect for ensuring user control and enforceability of policy in an accessible manner is to involve the user in the process of formulating policy, to achieve so far as possible consensus on a policy development to which the user has contributed. The user should be encouraged to express his or her views, to provide information that might be helpful to other stakeholders. The views of all stakeholders (users) should be carefully considered and they should be informed to what extent they have been taken into account or, if they haven't been, then why not.

---

[455] Security expert Bruce Schneier has commented, "We're not trading privacy for security; we're giving up privacy and getting no security in return." Schneier, Bruce, "Why Data Mining Won't Stop Terror", Wired News, 9 March 2005. http://www.schneier.com/essay-108.html

[456] The point is made in Čas, Johann, "Privacy in Pervasive Computing Environments – A Contradiction in Terms?", *IEEE Technology and Society Magazine*, Volume 24, Issue 1, Spring 2005, pp 24-33. http://www-personal.si.umich.edu/~rfrost/courses/SI110/paper_support/Cas,%20Privacy%20and%20Ubiquity.pdf

Needless to say, user control and enforceability of policy will work best in a transparent decision-making process, and we commend, as stated above, a formalised risk assessment – risk management process to that end.

In addition, we think industry initiatives, notably that of ARTEMIS platform, would be more successful if user concerns were recognised and taken into account through the participation of civil society organisations. Issues of privacy, identity management and digital divide should be considered by all working groups in academia and industry (which now is not the case) and that industry participants should not see regulatory concerns as barriers to be overcome, but as opportunities to ensure user acceptance of AmI. As the Commission has generally been promoting platforms as a means of strengthening European success in key areas, so the Commission could take the initiative to encourage the ARTEMIS participants to establish a working group devoted to the policy issues that have been the focus of the SWAMI project. This recommendation could also be applicable to other EC-inspired platforms.

5.9 CONCLUDING REMARKS – THE TOP SIX

This report has identified many threats and vulnerabilities and many safeguards for dealing with them. It does not pretend to be comprehensive. Our recommendations are not to be found only in this chapter (although it contains the main ones), but also in the chapter on safeguards.

Even though our report does not pretend to be comprehensive, perhaps we have identified too many safeguards or made too many recommendations, at least, in the sense that we have our doubts about how many officials in the Commission or in Member States or in industry and so on are going to systematically go through our proposed safeguards and recommendations, consider them and decide which are feasible, sensible or implementable.

We hope all of the stakeholder groups mentioned in this report do, at least, consider all of our safeguards and recommendations, but in the event that so many seem daunting, the SWAMI partners decided to prioritise them and the following our top six recommendations.

1. The Commission, together with Member States, perhaps under the auspices of ENISA should initiate a formalised risk assessment / risk management process with regard to the risks posed by AmI to security and privacy. We recommend that the assessment and decision-making process be open, transparent and inclusive, that stakeholder groups be identified and contacted and encouraged to take part in the process. Individuals should also be given an opportunity to express their views. Such a process could be initiated by means of a green paper on the risks to security and privacy in an AmI world. Whatever the outcome of the process, we recommend that the risk assessment be undertaken again (and again) in the future with some regularity, the periodicity of which might depend on the rapidity with which AmI is deployed (bearing in mind that the technologies for AmI are already being developed and deployed).

We also recommend that the precautionary approach be taken into account when developing and deploying new technologies. Such an exercise might be considered as a legal obligation.

2. The Commission and Member States should invest in an awareness campaign specifically focused on AmI, the purpose of which would be to explain to all stakeholders, but especially the public that AmI is on its way, that it offers great benefits, but also poses certain security and privacy issues. There are many ways of raising awareness (through education, the media, etc), but to give this recommendation some specific focus, we recommend that Member States hold an annual national contests which would offer some form of recognition to the best product or service offering privacy and security protection. We recommend a run-off at European level. This could be a counterpoint to the notorious bad publicity that ambient intelligence (especially RFID applications) has received in recent years.[457]

Any such campaign targeted at informing the public about ambient intelligence services and to inspire trust should involve *all* stakeholders and any such competition should be judged by independent evaluators.

3. The Commission and Member States should review carefully this report and, especially, section 4.4, to address the inadequacies and lacunae in the existing legal and regulatory framework with respect to AmI. Law is only one of the available tools for regulating behaviour, in addition to social norms, market rules and the "code", i.e., the architecture of the technology (e.g. cyberspace, ambient intelligence, mobile telephony…). The law can be a regulator on its own, but it can also regulate via influencing the "code" and other modalities of regulation.

The SWAMI consortium strongly recommends respecting this pluralism of modalities of regulation. In order to tackle the identified problems effectively, it is necessary to consider different approaches simultaneously.

4. The SWAMI consortium recommends that most of the challenges of new AmI environments be met by legal instruments that do not prohibit new technological developments, but channel them (such as by data protection and security measures). Transparency should be the default position, although some prohibitions referring to the political balances, ethical reasons or core legal concepts should be also considered in policy discussion. Focusing on concrete technologies rather than trying to produce general solutions seem to be more appropriate for AmI, an environment that adapts and responds to the changes of context, and in which privacy and other legal issues are also context-dependent. Thus, in developing policy options, one should focus on the concrete technologies, and apply channelling and prohibitive approaches accordingly.

5. The biggest weakness in enforcement of rights is the limitation of any European rule to Member States only, or to countries which have signed international conventions such as the Cyber Crime Convention). Clearly, ICTs and AmI have global dimensions. International cooperation in developing and enforcing the legal framework is necessary. Therefore, the Commission and Member States should be proactive in the development of

[457] RFID technologies and their promoters have received Big Brother Awards in various countries world wide. See e.g. http://bigbrotherawards.de/2003/.cop/; http://www.edri.org/edrigram/number4.3/frenchbba?PHPSESSID=a08c4d85ac916daab3d8660a1d377dd8; http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-187899; http://www.bigbrotherawards.cz/en/winners_2005.html

a more comprehensive international co-operation framework that would take AmI technologies and capabilities into account as a matter of urgency.

6. The European Commission should ensure that projects that it funds take questions of privacy, security and trust into account. Research programmes should contain a project line of accompanying measures covering the societal impact. Currently, EC calls say that project participants must conform to relevant EU legislation, inter alia, the data protection directive (95/46/EC). It is, of course, necessary that project participants (or any third party funded by the EC) conform to EU legislation, but we think the Commission should be more demanding – i.e., it should require those it funds to specifically speculate what privacy or security impacts might arise from their projects and what measures should be taken to address those. In other words, simply conforming to legislation is not enough. Project participants must be asked to foresee or even to speculate what privacy or security implications their projects *might* have. By the same token, the EC proposal and tender evaluators should also be asked to evaluate project proposals and tenders from the same optic. We recommend that Member States adopt a similar approach. We would like to especially emphasise the importance of funding research on technological safeguards for protecting privacy and enhancing security and for overcoming the digital divide. If technology does not provide solutions for human-technology interfaces for all, or for user-friendly security, other safeguards will not be able to solve the problem. We suggest that among technological safeguards research on intelligent algorithms is especially important.

As a final, parting comment for this report, the SWAMI partners believe that, sooner or later, we will live in a world of ambient intelligence. For ambient intelligence to be a success story, in human terms, according to democratic principles, and not to be an Orwellian world, all stakeholders must be cognisant of the threats and vulnerabilities and work together to ensure adequate safeguards exist. Certainly, industry should become more active in creating applications that are secure and privacy enhancing since this is the major way to create consumer trust and make ambient intelligence fruitful to *all* participants. Industry should not view privacy, security, identity, trust, and inclusion issues as regulatory barriers to be overcome. Rather, they should regard such measures as necessary, justified and, in the end, crucial to ensuring that their fellow citizens will use ambient intelligence technologies and services. In the meantime, we encourage all stakeholders to be vigilant.

6 REFERENCES

6.1 GENERAL

Aarts, E., R. Harwig and M. Schuurmans, "Ambient Intelligence", in P. Denning, *The Invisible Future: The Seamless Integration of Technology in Everyday Life*, McGraw-Hill, New York, 2002.

Ahmed, A. A. E., and I. Traore, "Anomaly Intrusion Detection based on Biometrics", *Proceedings of the 2005 IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY, June 2005.

Ailisto, H., E. Vildjiounaite, M. Lindholm et al., "Soft Biometrics – Combining Body Weight and Fat Measurements with Fingerprint Biometrics", *Pattern Recognition Letters*, vol. 27, 2006.

Ailisto, H., M. Lindholm, J. Mantyjarvi et al., "Identifying people from gait pattern with accelerometers", in E. M. Carapezza (ed.), *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IV*, Proceedings of the SPIE, 5779, 2005.

Alahuhta, P., M. Jurvansuu and H. Pentikäinen, *Roadmap for Network Technologies and Services*, Tekes, Helsinki, 2004. http://www.tekes.fi/julkaisut/Roadmap.pdf

Albrecht, Katherine and Liz McIntyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, Nelson Current publishers, Nashville, TN, 2005.

Alheit, K., "The applicability of the EU Product Liability Directive to Software", *The Comparative and International Law Journal of South Africa*, Vol. 3, no 2, 2001.

Alvestrand, H., "The Role of the Standards Process in Shaping the Internet", *Proceedings of the IEEE*, vol. 92, no. 9, 2004

Andrews, S., *Privacy and human rights 2002*, produced by the Electronic Privacy Information Center (EPIC), Washington DC, and *Privacy International*, London, 2002. *http://www.privacyinternational.org/survey/phr2002/*

ARTEMIS Strategic Research Agenda, First Edition, March 2006.
http://www.artemis-office.org/DotNetNuke/PressCorner/tabid/89/Default.aspx

Associated Press, "Spy Agency Removes Illegal Tracking Files", published in *The New York Times*, 29 Dec 2005.
http://www.nytimes.com/2005/12/29/national/29cookies.html

Axelrod, R., *The Evolution of Cooperation*, Basic Books, New York, 1985.

Bauer, M., M. Meints and M. Hansen, *Structured Overview on Prototypes and Concepts of Identity Management Systems*, FIDIS Deliverable D3.1, 2005.
http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf

BBC News, "Huge surge in mobile phone thefts", 8 January 2002.
http://news.bbc.co.uk/1/hi/uk/1748258.stm

Becher, A., Z. Benenson and M. Dornseif, "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks", in J. A. Clark, R. F. Paige et al. (eds.), *Security in Pervasive Computing*, Proceedings of the Third International Conference, SPC 2006, York, UK, 18-21 April 2006, Springer, Berlin, 2006, pp. 104-118.

Beck, U., A. Giddens and S. Lash, *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*, Stanford University Press, Stanford, 1994.

Bergstein, Brian, "Research Explores Data Mining, Privacy", The Associated Press, in *The Washington Post*, 17 June 2006.
www.washingtonpost.com/wp-dyn/content/article/2006/06/17/AR2006061700387_3.html

Beslay, L., and H. Hakala, "Digital Territory: Bubbles". Draft version available at http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf.

Beslay, L., and Y. Punie, "The Virtual Residence: Identity, Privacy and Security", IPTS Report 67. http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html

Bishop, Todd, "Gates tries to win over sceptics on security", *Seattle Post-Intelligencer*, 15 February 2006.
http://seattlepi.nwsource.com/business/259522_rsagates15.html

Blarkom, G. W. van, J. J. Borking and J. G. E. Olk (eds.), *Handbook of Privacy and Privacy-Enhancing Technologies*: The Case of Intelligent Software Agents, TNO-FEL, The Hague, 2003.

Bolt, David B., and Ray A. K. Crawford, *Digital divide: Computers and our children's future*, TV Books, New York, 2000.

Börjeson, Lena, Mattias Höjer, Karl-Henrik Dreborg, Tomas Ekvall and Göran Finnveden, "Towards a user's guide to scenarios - a report on scenario types and scenario techniques", Version 1.1b, Department of Urban Studies, Royal Institute of Technology, Stockholm, November 2005.
http://www.infra.kth.se/fms/pdf/ScenarioRapportVer1_1b.pdf.

Borking, J., "RFID Security, Data Protection & Privacy, Health and Safety Issues", presentation made during European Commission Consultation on RFID, Brussels, 17 May 2006.

Brey, Philip, "Freedom and privacy in Ambient Intelligence", *Ethics and Information Technology*, Vol. 7, No. 3, 2005, pp.157-166.
http://springerlink.metapress.com/(jpxudi2npzbwkp452b2mix55)/app/home/issue.asp?referrer=parent&backto=journal,2,28;linkingpublicationresults,1:103461,1

Brownsword, Roger, "Code, control, and choice. Why East is East and West is West", *Legal Studies*, Vol. 25 No 1, March 2005.

Burnett, R. and P.D. Marshall, *Web Theory: An Introduction*, Routledge, London 2002.

Čas, Johann, "Privacy in Pervasive Computing Environments – A Contradiction in Terms?", *Technology and Society Magazine*, IEEE, Volume 24, Issue 1, Spring 2005.

Clarke, R., "Information Technology and Dataveillance", *Communications of the ACM*, 31(5), May 1988.
http://www.anu.edu/people/Roger.Clarke/DV/CACM88.html

Committee on Information Systems Trustworthiness, *Trust in Cyberspace*, National Research Council, National Academies Press, Washington, DC, 1999.

Camenisch, J. (ed.), *First Annual Research Report*, PRIME Deliverable D16.1, 2005. http://www.prime-project.eu.org/public/prime_products/deliverables/rsch/pub_del_D16.1.a_ec_wp16.1_V1_final.pdf.

Cranor, L. F., "P3P: Making Privacy Policies More Useful", *IEEE Security and Privacy*, vol. 1, no. 6, 2003.

Creese, S., M. Goldsmith and I. Zakiuddin, "Authentication in Pervasive Computing", in D. Hutter, G. Müller et al. (eds.), *Security in pervasive computing*, First International Conference, Boppard, Germany, 12-14 March 2003, Springer, Berlin, 2003, pp. 53-70.

Custers, Bart, *The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen, 2004.

Daskala, Barbara, *Networks and Divides: A Digital Divide perspective*, London School of Economics and Political Science, MSc Dissertation, 2001.

Daugman, J., "Iris Recognition: Anti-spoofing Liveness Testing, Stable Biometric Keys, and Further Research Directions", in *BioSecure 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, European Commission, Seville, January 2005.

De Hert, P., "De soevereiniteit van de mensenrechten: aantasting door de uitlevering en het bewijsrecht" [Sovereignty of human rights: threats created by the law of extradition and by the law of evidence], Panopticon, *Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, Vol. 25, No. 3, 2004.

De Hert, P., "What are the risks and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection'*, No. 1, produced in January 2006 on behalf of the European Parliament, available through http://www.vub.ac.be/LSTS/pub/Dehert/006.pdf

De Hert, P., "European Data Protection and E-Commerce: Trust Enhancing?", in J.E.J. Prins, P.M.A. Ribbers, H.C.A. Van Tilborg, A.F.L. Veth & J.G.L. Van Der Wees (eds.), *Trust in Electronic Commerce*, Kluwer Law International, The Hague, 2002.

De Hert P. & F.P. Ölcer, "Het onschadelijk gemaakte Europees privacybegrip. Implicaties voor de Nederlandse strafrechtspleging" [The notion of privacy made innocent. Implications for criminal procedure], *Strafblad. Het nieuwe tijdschrift voor strafrecht*, Vol. 2, No 2, 2004.

De Hert P. & S. Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence" in *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Institute for Prospective Technological Studies - Joint Research Centre, Seville, July 2003.
ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf

De Hert, Paul, & Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in Erik Claes, Anthony Duff & Serge Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006.

De Hert, P. & S. Gutwirth, "Interoperability of police databases: an accountable political choice", to be published in *International Review of Law Computers & Technology*, 2006.

De Hert, P. & S. Gutwirth, "What are the risks and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection'*, No. 1. http://www.vub.ac.be/LSTS/pub/Dehert/006.pdf

Desai, M.S., J. Oghen and T.C. Richards, "Information Technology Litigation and Software Failure", *The Journal of Information, Law & Technology*, 2002 (2). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/desai/

Drees, Caroline, "Civil liberties debate leaves much of America cold", Reuters, published in *The Washington Post*, 18 May 2006.

Edler, J. (ed.), "Politikbenchmarking Nachfrageorientierte Innovationspolitik", Progress report No. 99, Office for Technology Assessment at the German Parliament, Berlin, 2006.

Espiner, Tom, "Viruses cause most security breaches", *ZDNet UK*, 28 Feb 2006.
http://news.zdnet.co.uk/0,39020330,39254929,00.htm.

Espiner, T., "Philips unfurls prototype flexible display", *ZDNet UK*, 2 Sept 2005.
http://news.zdnet.co.uk/hardware/emergingtech/ 0,39020357,39216111,00.htm

Espiner, Tom, "Florida spammer faces $11bn fine", *ZDNet UK*, 5 Jan 2006.

European Commission, "Electronic signatures: legally recognised but cross-border take-up too slow, says Commission", Press Release, 17 March 2006.

http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/325&format=HTML&aged=0&language=EN&guiLanguage=en

European Commission, "*e*Europe 2005: An Information Society for All. An Action Plan to Be Presented in View of the Sevilla European Council", COM (2002) 263 final. Brussels, 2002.

European Commission. "i2010 – a European Information Society for Growth and Employment", COM (2005) 229 final, Brussels, 2005.

European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, [31 May 2006]. http://ec.europa.eu/information_society/doc/com2006251.pdf

European Commission / Directorate General Information Society, *IST 2003: The Opportunities Ahead*, Office for Official Publications of the European Communities, Luxembourg, 2003.

European Commission, *eInclusion revisited: The Local Dimension of the Information Society,* Commission Staff Working Document, Brussels, 2005.

[European Commission] Impact Assessment: Commission Staff Working Document, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the EU Regulatory Framework for electronic communications networks and services, SEC(2006) 817, Brussels, 28 June 2006.
http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/public_consult/review/impactassessment_final.pdf.

European Data Protection Supervisor (EDPS), *Annual Report 2005*.
http://www.edps.eu.int/publications/annual_report_en.htm

European Group on Ethics in Science and New Technologies, "Ethical Aspects of ICT Implants in the Human Body", Opinion to the Commission, 16 March 2005.
http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf

Evers, Joris, "America 'must consider banning rootkits'", *CNET News.com*, 17 Feb 2006.

Faulkner, W., *Women, gender in/and ICT: Evidence and reflections from the UK*, Strategies of Inclusion: Gender in Information Society (SIGIS), Deliverable IST-2000-26329, 2000.

Federal Trade Commission (FTC), "FTC Releases Top 10 Consumer Fraud Complaint Categories", press release, 25 Jan 2006.
http://www.ftc.gov/opa/2006/01/topten.htm.

Friedewald, M., E. Vildjiounaite, D. Wright, I. Maghiros, M. Verlinden, P. Alahuhta, S. Delaitre, S. Gutwirth, W. Schreurs and Y. Punie, *The Brave New World of Ambient*

Intelligence: A State-of-the-Art Review, SWAMI Deliverable D1, July 2005. http://swami.jrc.es

Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005. http://www.fidis.net

Gehring, R. A., "Software Development, Intellectual Property, and IT Security", *The Journal of Information, Law and Technology*, 1/2003. http://elj.warwick.ac.uk/jilt/03-1/gehring.html.

Geist, Michael, "Sony's mea culpa: Copy-protection settlement lays groundwork for new laws", *The Ottawa Citizen*, 5 Jan 2006.

Gellman, Barton, "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans", *The Washington Post*, 6 Nov 2005.

Giddens, A., *The Consequences of Modernity*, Polity Press, Cambridge, 1990.

Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", *Netherlands Comparative Law Association*, 2002.
http://www.ejcl.org/64/art64-6.html.

Gillies, L., "European Union: Modified Rules of Jurisdiction for electronic Consumer Contracts", *Computer Law & Security Report*, Vol. 17 No. 6, 2001

Gillies, L., "A Review of the New Jurisdiction Rules for Electronic Consumer Contracts within the European Union", Commentary, *The Journal of Information, Law and Technology* (JILT), 2001 (1).
http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/gillies/

Gourova, Elissaveta, Christoph Hermann, Jos Leijten and Bernard Clements, *The digital divide - A research perspective. A report to the G8 Opportunities Task Force*. Technical Report EUR 19913 EN. DG JRC/IPTS, Seville, 2001. http://fiste.jrc.es/pages/detail.cfm?prs=708

Grabner-Kräuter, S., and E. A. Kaluscha, "Empirical Research in on-Line Trust: A Review and Critical Assessment", *International Journal of Human-Computer Studies*, Vol. 58, no. 6, 2003, pp. 783-812.

[GUIDE] Sociological study of IdM issues in Europe: Theoretical underpinnings, v.1, Deliverable 2.1.2.A, 17 December 2004.
http://istrg.som.surrey.ac.uk/projects/guide/documents.html

Günther, Oliver and Sarah Spiekermann, "RFID and the Perception of Control: The Consumer's View", *Communications of the ACM*, Vol. 48, No. 9, 2005.

Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham - Boulder - New York - Oxford, 2002, pp. 5-20

Gutwirth, S., "De polyfonie van de democratische rechtsstaat" [The polyphony of the democratic constitutional state] in M. Elchardus (ed.), *Wantrouwen en onbehagen* [Distrust and uneasiness], Balans 14, VUBPress, Brussels, 1998.

Gutwirth, S. & P. De Hert, "Regulating profiling in a democratic constitutional state", to be published in M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen*, to be published, submitted to Springer Press, Berlin, 2007.

Hafner, Katie, "After Subpoenas, Internet Searches Give Some Pause", *The New York Times*, 25 Jan 2006.

Hansell, Saul, "Increasingly, Internet's Data Trail Leads to Court", *The New York Times*, 4 Feb 2006.

Hansen, M., K. Köhntopp and A. Pfitzmann, "The Open Source Approach - Opportunities and Limitations with Respect to Security and Privacy", *Computers and Security*, vol. 21, no. 5, 2002.

M. Hansen and H. Krasemann (eds.), *Privacy and Identity Management for Europe*, PRIME White Paper, Deliverable 15.1.d, 18 July 2005. http://www.prime-project.eu.org/

Harmon, Amy, "Lost? Hiding? Your Cellphone Is Keeping Tabs", *The New York Times*, 21 Dec 2003.

Henderson, K., and A. Poulter, "The Distance Selling Directive: Points for Further Revision", *International Review for Law Computers & Technology*, Vol. 16 no. 3, 2002.

Hildebrandt, M. & J. Backhouse, *Descriptive analysis and inventory of profiling practices*, FIDIS deliverable 7.2, Brussels, 2005. www.fidis.net

Hildebrandt, M., & S. Gutwirth (eds.), *Profiling: Implications for Democracy and Rule of Law*, FIDIS deliverable 7.4, Brussels, 2005. www.fidis.net

Hildebrandt, M., "Profiles and correlatable humans", in N. Stehr (ed.), *Who Owns Knowledge?* New Brunswick NJ, Transaction Books, 2006.

Hildebrandt, M., and S. Gutwirth (eds.), *Implications of profiling on democracy and the rule of law*, FIDIS (Future of Identity in the Information Society), Deliverable D7.4, September 2005. http://www.fidis.net

Hilty, Lorenz, et al, *The Precautionary Principle in the Information Society, Effects of Pervasive Computing on Health and Environment*, Report of the Centre for Technology Assessment, February 2005.

HiSPEC, *Privacy Enhancing Technologies: State of the Art Review*, Version 1, HiSPEC Report, 2002.
http://www.hispec.org.uk/public_documents/7_1PETreview3.pdf.

Hoffman, Donna L., and Thomas P. Novak, "Bridging the Racial Divide on the Internet", *Science*, Vol. 280, 1998, pp. 390-391.

Hong, J. I., J. D. Ng, S. Lederer and J. A. Landay, "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems", in *Proceedings of Designing Interactive Systems (Dis2004)*, Boston, MA, 2004.

Hosein, G., "Threatening the Open Society: Comparing Anti-terror Policies and Strategies in the U.S. and Europe", *Privacy International*, London, 2005. http://www.privacyinternational.org/issues/terrorism/rpt/comparativeterrorreportdec2005.pdf.

Ihde, D., *Technology and the Lifeworld: From Garden to Earth*, Indiana University Press, Bloomington, 1996.

INDICARE Project, "Content Providers' Guide to Digital Rights Management: Any side effects in using DRM?". www.indicare.org

International Labour Organization, *ILO Seafarers' Identity Documents Biometric Testing Campaign Report*, Part 1, ILO, Geneva, 2004. http://www.ilo.org/public/english/dialogue/sector/papers/maritime/sid-test-report1.pdf

Institute for Prospective Technological Studies (IPTS), *Biometrics at the frontiers: assessing the impact on Society*, Study commissioned by the LIBE committee of the European Parliament, EC – DG Joint Research Centre, Seville, February 2005. http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf

ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*, First edition, International Organization for Standardization, Geneva, 1999.

ISO/IEC 17799:2005(E): *Information technology – Security techniques – Code of practice for information security management*. Second edition. International Organization for Standardization, Geneva, 15 June 2005. www.iso.org.

ISO/IEC 13335-1:2004: *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*, International Organization for Standardization, Geneva, 2004. www.iso.org

IST Advisory Group, K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten and J.-C. Burgelman, "Scenarios for Ambient Intelligence in 2010", Institute for Prospective Technological Studies (IPTS), EC-JRC, Sevilla, 2001.

IST Advisory Group (ISTAG), "Trust, Dependability, Security and Privacy for IST in FP6", Office for Official Publications of the European Communities, Luxembourg, 2002.

Jordan, Mary, "Electronic Eye Grows Wider in Britain", *The Washington Post*, 7 January 2006.

Julia-Barcelo, R., and K. J. Koelman, "Intermediary Liability in the E- commerce Directive: So far so Good, But It's not Enough", *Computer Law and Security Report*, Vol. 16, No. 4, 2000.

Kardasiadou, Z., and Z. Talidou, *Report on Legal Issues of RFID Technology*, LEGAL IST (Legal Issues for the Advancement of Information Society Technologies) Deliverable D15, 2006.

Keizer, Gregg, "Microsoft Helps Bulgaria Pinch 8 Phishers", *TechWeb News*, 23 January 2006. http://www.techweb.com/wire/security/177102753

Kent, Stephen T., and Lynette I. Millett (eds.), *IDs--Not That Easy: Questions About Nationwide Identity Systems*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academy Press, Washington, DC, 2002.

Kent, Stephen T., and Lynette I. Millett (eds.), *Who Goes There?: Authentication Through the Lens of Privacy*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, National Academies Press, Washington, DC, 2003.

Kerr, Jennifer C., "Credit Card Payment Co. Settles Charges", Associated Press, 23 Feb 2006.

Knospe, H., and H. Pohl, "RFID Security", in *Elsevier Information Security Technical Report*, vol. 9, No. 4, 2004.

Koorn, R., H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen and J. Borking, "Privacy-Enhancing Technologies. White Paper for Decision-Makers", The Hague, Ministry of the Interior and Kingdom Relations, 2004.
http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf

Koops, B.J. & M.M. Prinsen, "Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit" ["Glass house, transparent body. A future view on home law and body integrity"], *Nederland Juristenblad*, 12 March 2005.

Kravitz, D. W., K.-E. Yeoh and N. So, "Secure Open Systems for Protecting Privacy and Digital Services", in T. Sander (ed.), *Security and Privacy in Digital Rights Management,* ACM CCS-8 Workshop DRM 2001, Philadelphia, 5 Nov 2001, Revised Papers, Springer, Berlin, 2002.

Krebs, Brian, "Hackers Break Into Computer-Security Firm's Customer Database", *The Washington Post*, 19 Dec 2005.

Krebs, Brian, "Invasion of the Computer Snatchers", *The Washington Post*, 19 Feb 2006.

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

Krim, Jonathan, "Data on 3,000 Consumers Stolen With Computer", *The Washington Post*, 9 November 2005.

Kruger, Danny, *Access Denied? Preventing Information Exclusion*, Demos, London, 1998.

Kündig, A., *A Basis for IT Assessment. An overview of the underlying technologies, their applications and the implications for individuals, society and business*, Swiss Centre for Technology Assessment, 2002. http://www.ta-swiss.ch/www-remain/reports_archive/publications/2002/TA43_2002.pdf.

Lahlou, S., and F. Jegou, *European Disappearing Computer Privacy Design Guideslines* V1, Ambient Agora Deliverable D15.4, Electricité de France, Clamart, 2003. http://www.ambient-agoras.org/downloads/D15[1].4_-_Privacy_Design_Guidelines.pdf

Lahlou, Saadi, Marc Langheinrich and Carsten Rocker, "Privacy and Trust Issues with Invisible Computers", *Communications of the ACM*, Vol. 48 No. 3, March 2005.

Langheinrich, M., "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems", in G. D. Abowd, B. Brumitt and S. A. Shafer (eds.), *Proceedings of the Third International Conference on Ubiquitous Computing* (Ubicomp 2001), Springer-Verlag, Berlin, 2001.

Langheinrich, M., "The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects", Paper presented at the Designing for Privacy Workshop, DC Tales Conference, Santorini, Greece, 2003.

Lazarus, Wendy and Francisco Mora, *Online content for low-income and undeserved Americans: The digital divide's new frontier*, The Children's partnership, Santa Monica, 2000.

Leenes, R., and B.J. Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers & Technology*, Vol. 19, No 3, 2005.

Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

Lessig, Lawrence, "The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 133, 1999.

Lettice, J., "Carjackers swipe biometric Merc, plus owner's finger", *The Register*, 4 April 2005. http://www.theregister.co.uk/2005/04/04/fingerprint_merc_chop

Lettice, John, "Face and fingerprints swiped in Dutch biometric passport crack", *The Register*, 30 January 2006.
http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/

Lewis, Paul, "Court victory hailed as spam stopper", *The Guardian*, 28 Dec 2005.

Leyden, John, "Hackers cost UK.biz billions", *The Register*, 28 April 2004.
http://www.theregister.co.uk/2004/04/28/dti_security_survey/

Libbenga, Jan, "Video surveillance outfit chips workers", *The Register*, 10 Feb 2006.
http://www.theregister.co.uk/2006/02/10/employees_chipped

Lichtblau, Eric and James Risen, "Spy Agency Mined Vast Data Trove, Officials Report", *The New York Times*, 24 Dec 2005.

Luhmann, N., *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*, 4th ed., Lucius & Lucius, Stuttgart, 2000.

Magnus, U., and H.W. Micklitz, *Comparative Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services*: A study commissioned by the European Commission, Final Report, Part D: The Comparative Part, April 2004. http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf

Malone, Steve, "Google preps privacy defences", *PCPro*, 20 Feb 2006. http://www.pcpro.co.uk/news/83794/google-preps-privacy-defences.html

Markoff, John, "Voice Encryption May Draw U.S. Scrutiny", *The New York Times*, 22 May 2006. http://www.nytimes.com/2006/05/22/technology/22privacy.html?_r=1&oref=slogin

Meints, M., "AmI – The European Perspective on Data Protection Legislation and Privacy Policies", presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006. http://swami.jrc.es/pages/deliverables.htm (Report of the final conference)

Mohammed, Arshad, "Record Fine for Data Breach", *The Washington Post*, 27 January 2006.

Mohammed, Arshad, and Sara Kehaulani Goo, "Government Increasingly Turning to Data Mining", *The Washington Post*, 15 June 2006 http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html

Molas-Gallart, J., "Government Policies and Complex Product Systems: The Case of Defence Standards and Procurement", *International Journal of Aerospace Management*, vol. 1, no. 3, 2001.

Moores, T., "Do Consumers Understand the Role of Privacy Seals in E-Commerce?", *Communications of the ACM*, Vol. 48, no. 3, 2005.

Morino Institute, *From Access to Outcomes: Raising the aspirations for technology initiatives in low income communities*, Working Paper, Reston, VA, 2001. http://www.morino.org/divides/report.htm.

Müller, G., and S. Wohlgemuth (eds.), *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, 2005. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.3.study_on_mobile_identity_management.pdf.

Murray, Charles J., "Privacy Concerns Mount Over Retail Use of RFID", *EE Times*, 1 Dec 2003. http://www.techweb.com/wire/26803432

National Telecommunications and Information Administration (NTIA), *Falling through the net: Towards Digital Inclusion. A Report on Americans' Access to Technology Tools*, U.S. Department of Commerce, Economics and Statistics Administration, National Telecommunications and Information Administration, Washington, 2000. http://search.ntia.doc.gov/pdf/fttn00.pdf

Naylor, David, & Cyril Ritter, "B2C in Europe and Avoiding Contractual Liability: Why Businesses with European Operations Should Review their Customer Contracts Now", 15 September 2004. http://www.droit-technologie.org

Neuwrit, K., *Report on the protection of personal data with regard to the use of smart cards,* Report of Council of Europe (2001), accessible through http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents

Nissenbaum, H., "Securing Trust Online: Wisdom or Oxymoron", *Boston University Law Review*, Vol. 81, no. 3, 2001.

Nixon, M., J. Carter, J. Shutler and M. Grant, "New Advances in Automatic Gait Recognition", *Elsevier Information Security Technical Report*, vol 7, No. 4, 2002.

Norris, Pippa, *Digital divide: Civic engagement, information poverty, and the Internet worldwide*, Cambridge University Press, Cambridge and New York, 2001.

O'Brien, Timothy L., "Identity Theft Is Epidemic. Can It Be Stopped?", *The New York Times*, 24 Oct 2004.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development, Paris, 2001.

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Organisation for Economic Co-operation and Development, Paris, 2002.

OECD, *Report on Disclosure Issues Related to the Use of Copy Control and Digital Rights Management Technologies*, DSTI/CP(2005)15/FINAL, 2006. https://www.oecd.org/dataoecd/47/31/36546422.pdf.

Offe, C., "How Can We Trust Our Fellow Citizens?", in M. E. Warren, *Democracy and Trust*, Cambridge University Press, Cambridge, 1999.

Ofcom, *Online protection: A survey of consumer, industry and regulatory mechanisms and systems*, Office of Communications, London, 21 June 2006. http://www.ofcom.org.uk/research/technology/onlineprotection/report.pdf

Solove, Daniel J., *The Digital Person*, New York University Press, New York, 2004.

Olsen T., Mahler, T., et al, "Privacy – Identity Management, Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", LEGAL IST: LEGAL *Issues for the Advancement of Information Society Technologies*, Deliverable

D11, 2005. See LEGAL IST website http://193.72.209.176/default.asp?P=369&obj=P1076

Orr, R. J., R. Raymond, J. Berman and F. Seay, "A System for Finding Frequently Lost Objects in the Home", *Technical Report 99*-24, Graphics, Visualization, and Usability Center, Georgia Tech, 1999.

OUT-LAW News, "Sony BMG to settle 'rootkit' lawsuits", OUT-LAW.COM, 4 Jan 2006. http://www.out-law.com/page-6496

OUT-LAW News, "UK gov flies IT security kitemark", OUT-LAW.COM, 9 Sept 2005.

OUT-LAW News, "Children to be chipped in Mexico", OUT-LAW.COM, 13 Oct 2003.

Payne, C., "On the Security of Open Source Software", *Information Systems Journal*, vol. 12, no. 1, 2002.

Pennington, R., H. D. Wilcox and V. Grover, "The Role of System Trust in Business-to-Consumer Transactions", *Journal of Management Information System*, vol. 20, no. 3, 2004.

Perri 6 and Ben Jupp, *Divided by information? The "digital divide" and the implications of the new meritocracy*, Demos, London, 2001.

Pfizmann, A., and M. Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology*, Version v0.27, 20 Feb 2006. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

Pfitzmann, A. and M. Kohntopp, "Striking a Balance between Cyber-Crime and Privacy", *IPTS Report* 57, EC-JRC, Seville, Sept 2001. http://www.jrc.es/home/report/english/articles/vol57/welcome.htm

"Politie stuurt 3000 sms-berichten in onderzoek-Sévèke", Webwereld Newsletter, 21 March 2006, http://www.webwereld.nl/ref/newsletter/40348

Popitz, H., *Über die Präventivwirkung des Nichtwissens*, J. C. B. Mohr, Tübingen, 1968.

Prins, J. E. J., and M.H.M. Schellekens, "Fighting Untrustworthy Internet Content: In Search of Regulatory Scenarios", *Information Polity*, vol.10, 2005.

Prins, J.E.J., "The Propertization of Personal Data and Identities", *Electronic Journal of Comparative Law*, vol. 8.3, October 2004. http://www.ejcl.org/

Privacy International, "What is Wrong With Europe?", Media Release, 14 Dec 2005. The report is available at http://www.privacyinternational.org/comparativeterrorpowers or http://www.privacyinternational.org/issues/terrorism/rpt/comparativeterrorreportdec2005.pdf.

Punie, Y., "The Future of Ambient Intelligence in Europe: The Need for More Everyday Life", in R. Silverstone (ed.), *Media, Technology and Everyday Life in Europe: From Information to Communication*, Ashgate, Aldershot, UK, 2005.

Punie, Y., S. Delaitre, I. Maghiros and D. Wright (eds.), *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*, SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission, November 2005. http://swami.jrc.es.

Qinetiq, Transcrime and Interpol, *Future Threats and Crimes in the Ambient Intelligent Environment*, study for IPTS, 2005.

Ranneberg, K., "Multilateral Security: A Concept and Examples for Balanced Security", ACM New Security Paradigms Workshop, September 2000.

Reaney, Patricia, "Coming soon: Mind-reading computers", Reuters, 26 June 2006. http://today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006-06-25T232536Z_01_L23596655_RTRUKOC_0_US-SCIENCE-COMPUTERS.xml&archived=False

Reed, Ch., and A. Welterveden, "Liability", in Ch. Reed and J. Angel (eds.), *ComputerLaw*, London 2000.

Resnick, P. and R. Zeckhauser, "Trust Among Strangers in Internet Transactions: Empircal Analysis of eBay's Reputation System", in Michael R. Baye (ed.), *The Economics of the Internet and E-Commerce*, Vol. 11 of Advances in Applied Microeconomics, JAI Press, Amsterdam, 2002.

Resnick, P., R. Zeckhauser, E. Friedman and K. Kuwabara,. "Reputation Systems: Facilitating Trust in Internet Interactions", *Communications of the ACM*, 43(12), 2000, pp. 45-48. http://www.si.umich.edu/~presnick/papers/cacm00/reputations.pdf

Richtel, Matt, "Suddenly, an Industry Is All Ears", *The New York Times*, 4 March 2006.

Riegelsberger, J., M. A. Sasse and J. D. McCarthy, "The Mechanics of Trust: A Framework for Research and Design", *International Journal of Human-Computer Studies*, Vol. 62, no. 3, 2005.

Riguidel, M., and F. Martinelli, "Beyond the Horizon - Thematic Group 3: Security, Dependability and Trust", Report for Public Consultation, 2006. http://www.beyond-the-horizon.net.

Risen, James and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *The New York Times*, 16 Dec 2005.

Roussos, G., and T. Moussouri, "Consumer Perceptions of Privacy, Security and Trust in Ubiquitous Commerce", *Personal and Ubiquitous Computing*, Vol. 8, no. 6, 2004.

Samuelson, P., "Privacy As Intellectual Property?", *Stanford Law Review*, Vol. 52, 2000.

Sanders, Tom, "Microsoft unfolds next generation authentication", 15 Feb 2006. http://www.vnunet.com/vnunet/news/2150289/microsoft-unfolds-generation

Savvas, Antony, "Lax anti-virus practices fuel security fears", ComputerWeekly.com, 21 April 2005.

Schaub, M., *European Legal Aspects of E-commerce*, Europa Law, Groningen, Netherlands, 2004.

Schneier, Bruce, *Beyond fear*: Thinking sensibly about security in an uncertain world. Copernicus Books, New York, 2003.

Schneier, Bruce, "Identification and Security", *Crypto-Gram Newsletter*, 15 Feb 2004. http://www.schneier.com/crypto-gram-back.html.

Schneier, Bruce, "National ID Cards", *Crypto-Gram Newsletter*, 15 Apr 2004. http://www.schneier.com/crypto-gram-back.html

Schneier, Bruce, "Why Data Mining Won't Stop Terror", Wired News, 9 March 2005. http://www.schneier.com/essay-108.html

Schreurs, W., "Spam en electronische reclame [Spam and electronic communication]", *Nieuw Juridisch Weekblad,* 2003-48.

Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", to be published in M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen*, forthcoming, Springer Press, 2007.

Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS Deliverable D7.3, Brussels, 2005. www.fidis.net

Scott, A. O., "A Future More Nasty, Because It's So Near", Film review of "Code 46", *The New York Times*, 6 Aug 2004.

Sharpe, B., S. Zaba, and M. Ince, "Foresight Cyber Trust and Crime Prevention Project. Technology Forward Look: User Guide", Office of Science & Technology, London 2004.

[SIGIS], Strategies of Inclusion: Gender and the Information Society. http://www.rcss.ed.ac.uk/sigis/

Simon, K. D., "The Value of Open Standards and Open-Source Software in Government Environments", *IBM Systems Journal*, vol.44, no. 2, 2005.

Singsangob A., *Computer Software and Information Licensing in Emerging Markets, The Need for a Viable Legal Framework*, Aspen Publishers, 2003.

Sixtus, M., "Das Web sind wir", *Technology Review* (German Edition), Heft 3, July 2005.

Solove, Daniel J., *The Digital Person*, New York University Press, New York, 2004.

Sommer, Dieter, Architecture Version 0, PRIME Deliverable D14.2.a, 13 October 2004. www.prime-project.eu.org

Sorkin, David E., "Technical and Legal Approaches to Unsolicited Electronic Mail", *University of San Francisco Law Review*, Vol. 35, 2001.

Spiekermann, S., and F. Pallas, "Technology Paternalism – Wider Implications of Ubiquitous Computing", *Poiesis & Praxis*, Vol. 4, no. 1, 2006.

Spiekermann, S., and M. Rothensee, *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing*, Institut für Wirtschaftsinformatik, Humbold-Universität zu Berlin, 2005.
http://interval.hu-berlin.de/downloads/rfid/neuste%20forschungsergebnisse/SocioPsychofak.pdf

Stajano, F., "One user, many hats; and, sometimes, no hat – towards a secure yet usable PDA", *Proceedings of Security Protocols Workshop 2004*, Springer-Verlag, Berlin, 2004.

Stajano, F., and R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", first Security & Privacy supplement to IEEE Computer, April 2002.

Stajano, F., and J. Crowcroft, "The Butt of the Iceberg: Hidden Security Problems of Ubiquitous Systems", in Basten et al. (eds.), *Ambient Intelligence: Impact on Embedded System Design*, Kluwer, Dordrecht, 2003.

Stephanidis, Constantine, et al, "Toward an Information Society for All: HCI Challenges and R&D Recommendations," *International Journal of Human-Computer Interaction* 11, no. 1, 1999, pp.1-28.

Streitz, N. A., and P. Nixon, "The Disappearing Computer", *Communications of the ACM*, Vol. 48, no. 3, 2005.

Subirana, B., and M. Bain, *Legal Programming: Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond*, Springer, New York, 2005.

Summers, Deborah, "Bureau admits innocents branded criminals", *The Herald* [Scotland], 22 May 2006. http://www.theherald.co.uk/politics/62460.html

Sutter Gavin, "'Don't Shoot the Messenger?' The UK and Online Intermediary Liability", *International Review of Law Computers & Technology*, Vol. 17 No.1, 2003.

Tokyo Ubiquitous Network Conference, Chairman's Report, 2005.
www.itu.int/itu-wsis/2005/D-23chairmans_report.pdf

Tomlinson, Christine, "When Bush's Eavesdroppers Get a False Positive", *CounterPunch*, 9 Feb 2006. http://www.counterpunch.org/tomlinson02092006.html

Turow, Joseph, and Lilach Nir, *The Internet and the family 2000: The view from parents, the view from kids*, Annenberg Public Policy Center, University of Pennsylvania, 2000.
http://www.asc.upenn.edu/usr/jturow/Adobe%20I&F%202000%20fixed.pdf.

Van Dijk, Jan and Kenneth L. Hacker, "The Digital Divide as a Complex and Dynamic Phenomenon", *The Information Society*, Vol. 19, pp. 315-326, 2003. http://web.nmsu.edu/~comstudy/tis.pdf

Venkatesh, V., "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model", *Information Systems Research*, 11(4), 2000.

Vishwanath, A., "Manifestations of Interpersonal Trust in Online Interaction", *New Media and Society*, Vol. 6 (2), 2004.

Waelbroeck D., Slater D., and Even-Shoshan G [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.html

Warren, Samuel, and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. IV, No. 5 [15 Dec 1890].

Warwick, K., "Wiring in Humans", presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006. See Friedewald, M., & D. Wright (eds.), *Report on the Final Conference*, Brussels, 21-22 March 2006, SWAMI Deliverable D5, 2006. http://swami.jrc.es/pages/documents/Deliverable5-ReportonConference.pdf

Weiser, M., and J. S. Brown, "The Coming Age of Calm Technology", in P. J. Denning and R. M. Metcalfe (eds.), *Beyond Calculation: The Next Fifty Years of Computing*, Copernicus, New York, 1997.

Werther, "The Liberties of the Subject", *CounterPunch*, 17 Jan 2006. http://www.counterpunch.org/werther01172006.html

Wilkinson, Alec, "Taggers", *The New Yorker*, 20 Mar 2006.

Xenakis, C., and S. Kontopoulou, "Risk Assessment, Security & Trust: Cross Layer Issues", Special Interest Group 2, 2006.

Zeller, Tom Jr, "For Victims, Repairing ID Theft Can Be Grueling", *The New York Times*, 1 Oct 2005.

Zinnbauer, D. et al, *eInclusion Vision and Action: Translating vision into practice*, vision paper, IPTS, Seville, 2006.

6.2 LEGAL TEXTS

The Charter of Fundamental Rights of the European Union (2000/C 364/01)

Council of Europe - Cybercrime Convention of 23 November 2001

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

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

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.

Council Directive 90/385/EEC 0n the approximation of the laws of the Member States relating to active medical devices, *OJ* L 323, 26/11/1997.

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.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts *OJ* L 095, 21/04/1993.

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 on the free movement of such data, *Official Journal* L 281, 23 November 1995.

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.

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.

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.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *Official Journal* L 013, 19/01/2000.

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.

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.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic

communications sector (Directive on privacy and electronic communications) *OJ* L 201, 31/07/2002.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 , 13/04/2006 P. 0054 - 0063.http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

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.

Directive 98/27/Ec of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests, *OJ* L 166, 11/06/1998.

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) *OJ* L 108, 24/04/2002.

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.

6.3 OPINIONS OF ADVISORY BODIES

Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace 5401/01/EN/Final, WP 55, 29 May 2002.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf

Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data by means of Video Surveillance, 11750/02/EN WP 67, 25 November 2002.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_en.pdf

Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 30 May 2002, 5035/01/EN/Final WP 56.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

Article 29 Data Protection Working Party, Working document on biometrics, 12168/02/EN WP 80, 1 August 2003.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf

Article 29 Data Protection Working Party, Opinion on More Harmonised Information Provisions, 11987/04/EN, WP 100, 25 November 2004. http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp100/wp100_en.pdf.

Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 10107/05/EN WP 105, 19 January 2005.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Article 29 Data Protection Working Party, Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology 1670/05/EN, WP 111 28 September 2005.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf

Article 29 Data Protection Working Party, Working document on data protection issues related to intellectual property rights, WP 104, 18 January 2005.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf.

[EDPS] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004)835 final) *OJ C 181/27, 23 July 2005, 13-29.*

[EDPS] European Data Protection Supervisor, Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final), Brussels, 28 February 2006, 5 p. Available at http://www.edps.eu.int/legislation/Opinions_A/06-02-28_Opinion_availability_EN.pdf

[EDPS] European Data Protection Supervisor, Comments on the Communication of the Commission on interoperability of European databases, 10 March 2006. http://www.edps.eu.int/legislation/Comments/06-03

[EDPS] Opinion of the European Data Protection Supervisor, Annual Report, 2005, http://www.edps.eu.int/publications/annual_report_en.htm

European Group on Ethics in Science and New Technologies, "Ethical Aspects of ICT Implants In The Human Body", *Opinion to the Commission, 16 March 2005*. http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf

Working Party on the Protection of Individuals with regard to the processing of Personal Data, Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), XV D/5032/98, WP 11, 16 June 1998.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp11_en.pdf

ACKNOWLEDGEMENTS

SWAMI would like to thank the following experts for their participation in the SWAMI Work Package 3 Workshop, November 29, Brussels, 2005.

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

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

Jan Möller, Independent Data Protection Centre Schleswig-Holstein, Kiel, Germany;

Michael Vanfleteren, KU Leuven, Belgium.

Norbert Streitz, Fraunhofer IPSI, Darmstadt, Germany

Lorenz Hilty, Swiss Federal Materials Testing Agency, St. Gallen, Switzerland

Marc Langheinrich, ETZ Zürich, Switzerland

Sandro Bologna, Italian National Agency for New Technologies, Energy and the Environment, Rome, Italy

Marco Conte, CE Consulting, Rome, Italy

Maddy Janse, Philips Research, Eindhoven, The Netherlands

Michael Lyons, BTexact Technologies, Ipswich, United Kingdom

Bart Walhout, Rathenau Instituut, The Hague, The Netherlands

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.

Deliverable Summary Sheet

Project Number:	IST-2004-006507
Project Acronym:	SWAMI
Project title:	Safeguards in a World of Ambient Intelligence
Deliverable no.:	3
Due date:	March 2006
Delivery date:	July 2006
Delivery status:	Public
Work package no.:	3
Leading partner:	Fraunhofer Institute for Systems and Innovation Research, Trilateral Research and Consulting
Contributing partners:	All
Partners owing:	All
Distribution Type:	Public