FIDIS

Future of Identity in the Information Society

Title:	"D12.2: Study on Emerging AmI Technologies"
Author:	WP12
Editors:	Mark Gasson (University of Reading, UK) Kevin Warwick (University of Reading, UK)
Reviewers:	Eleni Kosta (K.U. Leuven, Belgium) Martin Meints (ICPP, Germany)
Identifier:	D12.2
Type:	[Deliverable]
Version:	1.0
Date:	Monday, 01 October 2007
Status:	[Final]
Class:	[Public]
File:	FIDIS_D12.2_v1.0.doc

Summary

The technical issues relating to the actual implementation and thus realisation of Ambient Intelligence (AmI) environments are immense, and in most cases tangible solutions to technical related problems are still yet to be found. Meanwhile, 'Emerging Technologies' has become a term which considers the convergence of areas such as nanotechnology, biotechnology, information technology, cognitive science, robotics, and artificial intelligence. Here we discuss how technologies which stem from this idea of domain fusion can be considered appropriate in the fabric of an AmI environment, meaning that AmI may actually be an application area made possible through this new emerging technology phenomenon. Further, we assess some of the emerging technologies on the basis of the European Charter of Fundamental Rights and Freedoms and apply an 'infoethic' approach (the application of ethical principles to the development and use of information and communication technologies) to raise questions regarding the role of fundamental rights for emerging technologies. Additionally, we offer a forum for an initial inter-disciplinary debate based on the complex issue of technology evolution in its wider socio-cultural context through the use of an initial anthropological statement, and subsequent domain orientated replies. In essence, this deliverable is less about firm answers to specific questions, and instead aims to inform the reader on how emerging technologies may find application in AmI, and to stimulate further discussion on both the specific and broader issues that such development entails.

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	20.02.2007	Initial release with technical and social chapters
0.2	26.03.2007	Integration of social replies
0.3	12.04.2007	Integration of legal chapter
0.4	21.05.2007	Editing, conclusions and summaries
0.5	13.06.2007	Initial release for internal review
0.6	25.07.2007	First reviewer revisions
0.7	03.08.2007	Second reviewer revisions
0.8	18.08.2007	Further integrative editing
0.9	13.09.2007	Final minor revisions
1.0	28.09.2007	Final version

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
2 Introduction	Editors
3 Emerging Technologies for AmI	Mark Gasson, Martin Meints, Stefan Köpsell & Vassiliki Andronikou
4 Fundamental rights and emerging technologies	Wim Schreurs, Bert-Jaap Koops & Colette Cuijpers
5 Emerging Technologies and Society	Daniela Cerqui, Eleni Kosta, Diana Bowman, Bert-Jaap Koops, Stefan Köpsell, Martin Meints & Mark Gasson
6 Conclusion	Editors

Table of Contents

1 Executive Summary

The technical issues relating to the actual implementation and thus realisation of Ambient Intelligence (AmI) environments are immense, and in most cases tangible solutions to technical related problems are still yet to be found. This situation leads to some interesting points of debate on technical, legal and wider societal levels. Firstly we have to consider where these AmI enabling technologies will evolve from. 'Emerging Technologies' has become a term which considers the convergence of areas such as nanotechnology, biotechnology, information technology, cognitive science, robotics, and artificial intelligence. Such technologies which stem from this idea of domain fusion can be considered appropriate in the fabric of an AmI environment, meaning that AmI may actually be an application area made possible through this new emerging technology phenomenon.

Here we present a non-exhaustive range of 'emerging' technologies, stemming from fundamental sensor technology for AmI spaces which will enable the data capture from which new 'profile' information can be inferred, to enabling technology, i.e. technology which will serve in the underpinning infrastructure to provide the networking and processing capabilities necessary in the envisaged future scenarios of augmented living. Because, in large, these technologies are not at a mature stage in their development, we discuss the theoretical workings and point to how they may indeed find application in AmI spaces.

The development of such technologies clearly has the potential for wide ramifications in our everyday lives, and in fact while the technology is sill in its development phase is an ideal time to debate their likely impact. Indeed, because of the fast development in technology and the unstoppable experimentation in society itself, the traditional mechanisms of law – that work via policy makers or legal politicians – typically only intervene at the moment a particular technology with all its short-term advantages at a micro-level has been put in the market. As such, the intervention with regard to the possible negative impact on a long term macro-level, should, in order to be effective, not be purely legal at a post-production level but should also take place in an earlier stage. Thus, this can only be achieved by actions that go beyond law alone. 'Infoethics' is the application of ethical principles with regard to the development and use of information and communication technologies and here, in the context of the technologies presented, we investigate one part of this broad field: the role of fundamental rights for emerging technologies.

Additionally within this deliverable, we offer a forum for an initial inter-disciplinary discussion based on the complex issue of this technology evolution in its wider socio-cultural context. Technology mirrors social and cultural values, if only because technology developers do not operate in a vacuum, but in the broader social and cultural context. By offering one anthropological viewpoint of this dependency and inviting replies from researchers within both the technical and legal domains, we hope to further stimulate discussion on this broader topic.

In essence, this deliverable is less about firm answers to specific questions - indeed to a large extent it would be too presumptuous to do so. Instead it aims to inform the reader on how emerging technologies may find application in AmI, and to stimulate further discussion on both the specific and broader issues that such development entails. This deliverable is seen as an initial investigation into areas less explored by FIDIS from which further and more specific work may derive, for example D12.6 'Study on ICT implants'.

2 Introduction

Technology exists as a means to further empower people, a result that is best achieved by constructing a close synergy between man and machine. The rapid development of technology has led to new fields of research dedicated to developing new and intuitive methods by which humans can interact with machines. Essentially, the problem is no longer just one of how technology can make a task easier for us, but in addition how we can interact with machines to benefit from their functionality to the greatest extent. It is now possible for machines to greatly augment our existing capabilities. Indeed an electronic organiser can be viewed as a method of augmenting our own memory, however laboriously pursuing the required information by prodding at an array of buttons as the interface between our cognitive abilities and the device's memory capabilities does little to do it justice. Essentially, traditional interfaces underexploit the processing potential of both the user and technology. This is true for both the input and output interaction processes in the traditional interaction paradigm, that is, instructing the machine to perform a task and the machine relaying back to the user new information regarding what it has done or what it is doing.

Essentially, the interface through which a user must interact with the machine provides a distinct layer of separation between what the user wants the machine to do, and what it actually does. Certainly, this separation imposes a cognitive load upon the user that is directly proportional to the level of difficulty the user experiences [Turk (2000)]. Manual intention through joystick, button or keyboard operation, 'point & click' operations via the mouse and recently voice recognition are perhaps the most widely used methods of interaction. Intuitively however, it would seem that these traditional interfaces greatly underexploit the processing capabilities of the user by presenting a bottleneck in the link between thinking what we want to happen, and laboriously pursuing those actions. Indeed, the fundamental issue can be viewed as two powerful information processors (human and machine) attempting to communicate with each other via a narrow bandwidth, highly constrained interface [Tufte (1989)]. Even the seemingly advantageous voice recognition interface has the additional payload of utilising parts of the brain that are employed for general problem solving to formulate sounds into words [Shneiderman (2000)], i.e. the cognitive load is increased when the thought has to be spoken.

Technological development moves towards exploitation of all sensory modalities to allow humans the ability to receive information from machines to the fullest extent. Currently, by far the most ubiquitous example is that of visual display screen, even though purely visual information alone is not optimum. Wearable computers have been proposed as a possible solution, although the first and still most common implementation is the head mounted display which optically overlays computer generated information on a real world scene [Mann (1997)]. This Augmented Reality (AR) is viewed as a halfway between Virtual Reality (VR) and telepresence since, whereas VR completely immerses the user inside a synthetic environment, AR either superimposes or composites virtual objects visually or audibly [Cohen *et al.* (1999)] on the real world, allowing virtual and real objects to coexist in the same space. However, AR has yet to supply interactivity rich enough to merge the real and virtual domains seamlessly. This is in part due to a lack of sensory modalities being exploited resulting in a very low level of achievable tangibility.

Ambient Intelligence Environments (AmI) have been presented for many years as the panacea for the human / technology interaction bottleneck. The very essence of AmI is to enrich the user experience by capitalising on the potential that additional computing processing can bring. Part of this enrichment is achieved by augmenting the user in their daily lives through additional services and access to additional information. *However*, this is achieved whilst actually reducing the focus on the traditional explicit data input / output paradigm - a true shift in our concept of what a computer is, and how we should interact and use it.

"*It seems like a paradox but it will soon become reality: The rate at which computers disappear will be matched by the rate at which information technology will increasingly permeate our environment and our lives*" [Streitz & Nixon, (2005)].

2.1 This Deliverable

The goal of this deliverable is to analyse supporting and enabling technologies for identity and identification which will play a central role for future implementations of profiling in AmI (as extensively discussed in FIDIS WP7). Therefore the following explanations have to be read with the context and concepts of AmI in mind. Nevertheless some of the selected technologies and their impact on identity, identification and, more generally speaking, on privacy will also be explained using examples from other fields of application. This is especially done when it helps the reader to more easily understand the problems arising from a given emerging technology.

As stated in FIDIS D7.3 ***profiling is an essential part of the idealised AmI***, and according to the findings of D7.2 the process of automated profiling includes:

- recording and storing of data, and
- identifying patterns and trends in the data (by running algorithms through the databases)

In a report of the Winter Corp. [Winter *et al.* (2006)] the growth of database size was analysed based on surveys. They not only found that in 2004 the largest system in the world (100 terabyte of data) was 100 times larger than in 1995 (1 terabyte of data), but they also identified that the "database size is growing at a staggering rate"[1]. Moreover the report emphasises ongoing demands on the scalability of databases in terms of query complexity and volume, number of users and data latency (summarised as multidimensional scalability).

Putting all this together the world of an idealised AmI requires emerging technologies, which are able to *store huge amount of data* and offer *nearly unlimited computing power*. Both have to be available in every place which wants to implement ambient intelligence. Even if we

[1] Of course these numbers only emphasise lower bounds on the growing manner of databases as not every organisation wants to publish the sizes of their databases.

take Moore's law[2] into account, it cannot be foreseen that this would be possible in an economic manner without decoupling the places where these resources are needed and the actual locations of the sources of them. This simply arises from the fact that the demand increases at least at the same rate as the available resources increase. In other words: the envisaged AmI café-bar would need a computing centre in its cellar.

This problem can theoretically be solved by using the following (emerging) technologies:

- **grid computing,** which can provide the necessary computing power and storage capacity without the need to install extensive hardware in the places where the computing power is needed, and
- **peer-to-peer based network architectures,** which can be used to economically transfer the huge amount of collected data to the processing elements of the grid

Both technologies are not 'emerging' in terms of only recently being mentioned in the literature. However, their practical usage is still far behind its potential. Especially the vision of grid computing, to make computer power as easy to access as an electric power grid, is still just a vision[3]. Nevertheless both technologies have made big steps toward their goals so that one can conclude that they are still in their 'emerging' state. Moreover the usage of these technologies in the field of AmI (which in itself is an emerging technology) is a new approach which could raise them to a new level, if AmI becomes a real success.

Linked to this are a wide range of "emerging" identity and identification, privacy and data protection related problems. They are to some degree inherently present in the aforementioned technologies, but using them in the context of AmI would dramatically increase their quality and quantity as well as their impact on society at large. Details of these technologies are discussed in section 3.3, whilst the implications from a legal perspective are discussed in section 4.3.

Besides the basic capabilities to process huge amounts of data quickly, there is a need for technologies which deal with the problem of exactly *how* this processing should be done. In the field of AmI, there is one notable area of research that addresses context awareness and context aware systems. Although it is controversial among researchers *exactly* what context awareness actually means, it is fair to say that a context aware system is able to perceive its environment[4] and bases its (algorithmic) decisions on this perception. In FIDIS deliverable D7.3 this was called "environmental awareness" and identified as a central aspect of AmI. More details on context awareness and context aware systems are given in section 3.3.6.

[2] Moore's Law is the empirical observation that the number of transistors on an integrated circuit for minimum component cost doubles every 24 months, implying an exponential growth in the complexity of information processing technologies.

[3] For example see the Business Experiments in GRID (BEinGRId) project.

[4] Here *environment* really means the spheres which surrounds the system and are outside of them. Note that this is different to the typical understanding of the term "environment" in the area of computing and software systems.

The existence of huge amounts of data has been identified as a necessary basis for AmI and has been assumed to pre-exist. But in fact in the AmI world new data are constantly collected using all kinds of sensors. As identified in FIDIS deliverables D7.2 and D7.3 the ubiquitous presence of sensors (as envisioned in basic AmI scenarios) leads to high risk for privacy and threats on the protection of personal data. The fundamental problem would be a problem of control - especially the control of the end user about his personal data. D7.3 discusses some technical measures to overcome that problem. Although the listed mechanisms demonstrate that service providers do not necessarily need to collect and store huge amounts of personal data to provide sophisticated AmI spaces, there is no solution inherent way to prevent them from collecting and processing the data. Therefore new emerging technologies are needed to solve this problem. One prerequisite for this kind of new technology is some means (e.g. sensors) which are able to detect sensors. Details of emerging trends in sensor technologies and the resulting applications can be found in section 3.2, whilst section 3.2.8 specifically presents details on such sensors which detect sensors and gives a broader overview how this technology could be used to solve privacy problems with the AmI world. Further legal discussion is given in section 4.3

2.1.1 Emerging Technologies and Society

Both emerging and converging technologies describe the emergence and convergence of new and potentially disruptive technologies. These address areas such as nanotechnology, biotechnology, information technology, cognitive science, robotics, and artificial intelligence. Advocates of the benefits of technological change typically see emerging technologies as offering hope for the betterment of the human condition. However, critics of the risks of technological change, and even some advocates, warn that some of these technologies could pose dangers. In some scenarios, it is considered that these could even contribute to the extinction of humanity itself.

Clearly we have adopted a technologically mediated way of living which inherently has far reaching consequences. Here we offer a forum for an initial inter-disciplinary discussion based on the complex issue of this technology evolution in its wider socio-cultural context. Following an initial statement on the topic from an anthropological perspective, we invite the responses of individuals and groups from the technical and legal disciplines. In this way we hope to contribute to the growing debate on the wider implications of emerging technology for our (continued) way of life.

3 Emerging Technologies for AmI

3.1 Introduction

The technical issues relating to the actual implementation and thus realisation of Ambient Intelligence (AmI) environments are immense, and in most cases tangible solutions to technical related problems are still yet to be found. However, although concrete solutions are yet to be realised, the theoretical problems which must be overcome are largely documented. Being able to profile a user within the AmI space is key to its success and as such the technological infrastructure which can allow this process is essential.

In a general sense, the technical issues of profiling in AmI fall into two broad categories: data collection, and data processing. FIDIS deliverable D7.2 examined the data mining techniques which could be adopted for the purpose of creating a profile from previously collected data. This chapter highlights technical infrastructure issues which relate to the problem of data collection for profiling in AmI, i.e. the technical infrastructure that needs to be present to allow the profiling activity to take place. Such issues revolve significantly around interoperability achieved through standardisation of hardware and software elements of the AmI. Whilst this does not encapsulate all related problems, the aim here is to simply place technical aspects in context with profiling and so broader technical issues of the AmI infrastructure are out of the scope of this document. Such broader issues may become the subject of subsequent FIDIS deliverables, however, further information on the subject of interoperability can be found in FIDIS deliverable D4.1.

3.1.1 The essence of AmI

AmI itself will not be the outcome of any single technology or application; rather it is an 'emergent' property.[5] Essentially, AmI is more than just the sum of its parts. Ubiquitous Computing is the next wave of technology, a paradigm shift from our current relationship with technology, whereby many thousands of wireless computing devices are distributed in the environment in everyday objects around us. Clearly this technology integration into the environment is a key aspect of AmI. Ubiquitous Communication will allow robust, *ad-hoc* networks to be formed by this broad range of mobile and static devices, forming a ubiquitous system of large-scale distributed networks of interconnected computing devices. By adding intelligent user interfaces and integrating sensing devices, it should be possible to identify and model user activities, preferences and behaviours, and create individualised profiles. These key aspects are all required to achieve the ideal AmI Environment.

As mentioned previously, the aim of the AmI environment is to provide a context aware system, using unobtrusive computing devices that will improve the quality of people's lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf. To achieve this, the 'intelligent' environment, or rather an intelligent *agent* within the environment needs to build up a profile of each individual, and be able to subsequently link the profile with the correct individual. In essence, *the environment itself has become the interface to the distributed, seamless and invisible AmI*. In a world where computing is truly ubiquitous, the environment will actually monitor the direct interaction of people with objects, and profiles will seamlessly follow the individual to whom it is linked.

[5] ISTAG, "Ambient Intelligence: From vision to reality. For participation - in business & society", 2003.

3.1.2 AmI Infrastructure

The concept of AmI provides a wide-ranging vision of how the Information Society will develop. Certainly, the emphasis of AmI is on greater user-friendliness, more efficient services support, user- empowerment, and support for human interactions. To fulfil this scenario, the following major technological research clusters have been proposed, which are deemed a necessary requirement for the AmI vision:[6]

- **AmI compatible enabling hardware:** including fully optical networks, nano-micro electronics, power and display technologies
- **AmI open platforms:** for interoperating networks based upon a corporate effort to define a 'service control platform'
- **Intuitive technologies:** involving efforts to create natural human interfaces
- **AmI developments in support of personal and community development:** including socio-technical design factors, support for human to human interaction and the analysis of societal and political development
- **Meta-Content services developments:** to improve information handling, knowledge management and community memory, involving techniques such as smart tagging systems, semantic web technologies, and search technologies
- **Security and trust technologies:** in support of privacy, safety, and dependability.

The AmI infrastructure is built on the notion that *ad-hoc*, complex, heterogeneous networks can function and communicate in a seamless and interoperable way. Only in this way can the broad range of services envisaged be offered to the individual. Essentially, the AmI is expected to embrace the *heterogeneity* arising from the different network technologies such that it appears *homogeneous* to the user. The vision is to allow for co-operation between networks on demand and without the need for offline negotiation between network operators.

The importance of this was underlined by the ISTAG, who identified three key breakpoints for AmI development. Notably, the first of these is:

"… under the requirement that AmI calls for a very flexible and seamless interoperation of many different devices on many different networks, it is a *key requirement that there is a set of common platforms or de facto standards to permit this interoperation to take place*."

The group felt that this would either be achieved through a deliberate effort to develop such open platforms or would arise from proprietary pacts between industrial suppliers.

[6] ISTAG, "Scenarios for ambient intelligence in 2010", 2001, available at: http://cordis.europa.eu/ist/istag.htm

3.2 AmI through Emerging Technologies

Emerging Technologies has become a term which considers the convergence of such areas as nanotechnology, biotechnology, information technology, cognitive science, robotics, and artificial intelligence. While previous FIDIS deliverable such as D7.7 ('Report on AmI, profiling and RFID') have explored how we can actually apply artificial intelligence techniques to large datasets to 'find' new information, here we look at the fundamental technologies which may be used in an AmI scenario for capturing and handling the data from which this knowledge may be drawn. Such technologies appear to stem from this idea of domain fusion, meaning that AmI may actually be an application area made possible through this new emerging technology phenomenon.

3.2.1 Simple Sensors

Typically, sensors are simple devices which monitor single variables. They are not 'smart' as such, and thus produce data (i.e. numbers and values) rather than information (i.e. what the numbers and values actually mean in their context). However, the combined pool of data from multiple sensors can be used to infer new information. For example, knowing one physiological attribute of a person may lead to several interpretations of that person's current psychological state. However, the combined resources of multiple types of sensor, perhaps reading heart rate, body posture, hormone levels, skin temperature and galvanic resistance may lead to more accurate estimation of emotional state. This in essence is at the heart of technologies such as affective computing (see section 3.2.3) which can self-adapt based on the user's attitude and mental state.

By augmenting an environment with simple sensors, the 'pool' of data is increased. Technology developments, especially in the field of material science, are making a new generation of simple and low cost sensors a reality, and indeed augmentation of these devices through nano, information and communication technologies will lead to a new wave of smart sensor devices.

3.2.2 Radio Frequency Identification

Although currently utilised in many incarnations, RFID technology has far from reached maturity. The workings and some of the associated issues of RFID have been discussed at length in several other FIDIS deliverables (for example see D3.6, D3.7, D7.7 and D12.3) so will not be re-iterated here. However, RFID has undoubtedly become inherently associated with AmI as an enabling technology because it fulfils several of the key requirements, most notably those of cost and power, meaning highly redundant numbers of unobtrusive devices can be located within an environment. In brief, RFID tags wirelessly communicate data to reader devices, from which typically the power is supplied wirelessly to the tag. The data, in the simplest devices, is a unique code which identifies the tag, and thus the object, if known, to which it is attached.

One of the key advantages to RFID is the prospect that such tags will be embedded in all objects within an environment because there are varying advantages to doing so. These range from ease of stock taking, logistics, product shipping to security and indeed simply identification. Thus if one buys a product that is equipped with an RFID tag for shop security purposes, then unless it is destroyed on purchase, the tag makes the product a uniquely identifiable object within an environment. Moreover, if the AmI is able to conclude what a

new object is through the context in which it is interacted with, then this is additional information further exploitable by the dynamic environment.

3.2.3 Software Agents

Research with respect to software agents started in the late 1980s. Today, software agents are mainly understood as programs that are able to work independently (autonomous), are able to react to changes in their environment (reactive), are able to act proactively and can communicate with other software agents. In the early 1990s the term "software agents" was used quite broadly, covering different areas of research in software technology. To focus the broad use of the term Nwana (1996) suggested a typology for software agents that is still being used.

It has been suggested to use software agents for many routine like works such as complex searches for information in libraries and network attached storages and processing of (digital) products in e-commerce (see for example [Jennings & Wooldridge (1996)]). Software agents on one hand need context awareness to understand e.g. the will of its user, on the other hand they need a certain type of "intelligence" to be able to make decisions. An important area of use for software agents today are simulations in science and computer games. In this context a number of highly specialised agents have been developed and are in use.[7]

Software agents may play a major role in ambient intelligent environments to search autonomously for information, to evaluate them and to draw conclusions including adaptive decision making.

Research in software agents is carried out in the private sector (mainly enterprises) and by public research institutions (mainly universities) world wide. In Europe coordination of stakeholders is supported by the EU in the context of the IST program (project AgentLink[8]).

3.2.4 Affective Computing

In recent years there has been much diverse work which explores the use of computing in ways which involve human emotion. This area is commonly referred to as *affective computing*. This includes work on the use of emotions in human-computer interaction, Artificial Intelligence (AI) and agent architectures which are inspired by the mechanisms of emotion, the use of emotion in computer-mediated communication, the study of human emotion through computers and philosophical issues concerning, for example, the extent to which it is meaningful to talk about emotion in computational terms.

In psychophysiology there lies an assumption that all human behaviour, including perception, cognition, emotion, and action, has a physiological substrate. Thus, it may be possible to identify reliable physiological indicators of psychological states and personality. The idea that these can be 'reliable' comes from an understanding of the autonomic nervous system (ANS). Typically we are unaware of our ANS because it functions largely involuntarily, via sympathetic (giving us fight and flight responses) and parasympathetic (which for example allow resting and digesting) pathways. The ANS is thus ultimately responsible for involuntary

[7] See http://en.wikipedia.org/wiki/Software_agent

[8] See http://www.agentlink.org/

physical effects associated with emotions such as anxiety, fear, anger, embarrassment, and joy, and the heightened mental focus associated with concentration and problem solving. If we are able to interpret the physical, and thus readily measurable, changes and states, then we should be able to deduce some of the underlying emotional states.

The physiological measures most often studied for relations to psychological state are electroencephalograms (EEG), skin conductance, heart rate, blood pressure, skin temperature, respiration, muscle tension, and eye movements (see [Lisetti & Nasoz, (2004)] for a review of research). Sensor technologies have been developed in all these cases, and indeed small wearable technologies, which incorporate them, are technically feasible. However, one of the most vigorously researched measures is currently that of EEG because it is considered a potentially richer source of information, and because changes are more immediate than in other physiological recordings, for example see [Berka *et al.* (2004)].

3.2.5 Brain Computer Interfaces

Traditional Brain Computer Interfaces (BCIs) are typically designed to respond to specific patterns detected in spatiotemporal electroencephalograms (EEG) measured non-invasively from the scalp, see [Wolpaw *et al.* (2002)] for a review. The EEG signal originates from the electrical activity of thousands of neurons in the brain, but can be viewed as a mixture of five distinct frequency spectra of note: Alpha, Beta, Theta, Delta and Mu waves, an important property since each represents activity associated with different conscious or unconscious states.

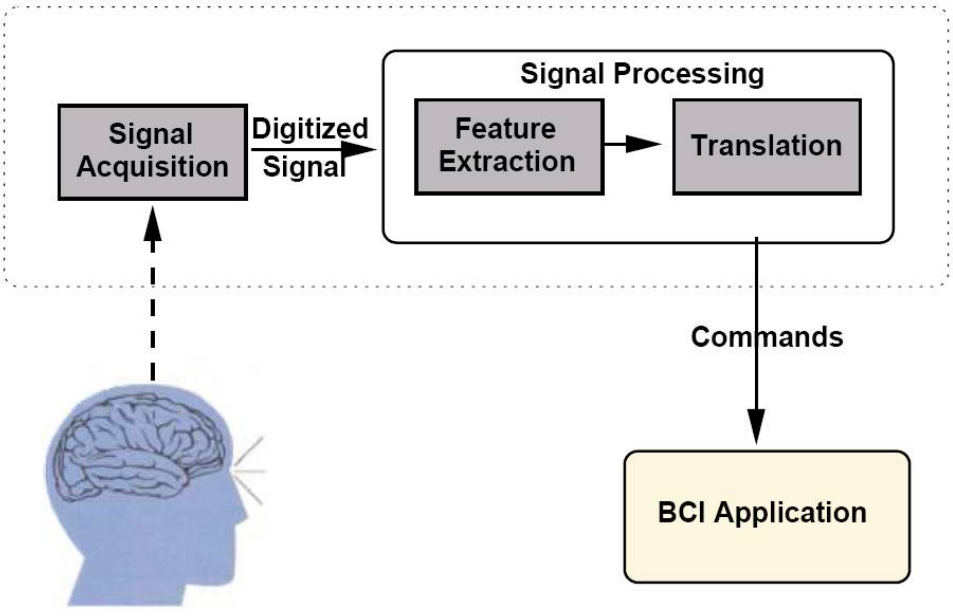

Figure 1: Basic block diagram of a BCI system incorporating signal detection, processing and deployment [Thorpe *et al.* 2005]

In current implementations, BCI based systems generally allow the user to select characters or icons from a screen by either moving a cursor or halting a scrolling list of options. However, the problem of generating a suitable EEG control signal and subsequently detecting it is a non-trivial one. With theory and methods drawn from a vast array of disciplines, this area of

research has developed a substantial nomenclature. One method is to correlate specific movements, or thoughts of movements with particular patterns in the EEG signal [Bozorgzadeh *et al.* (2000) & Lusted and Knapp (1996)]. Another is to train the user to control the amplitude of their Beta or Mu waves (associated with an alert state of mind and the motor cortex respectively) in order to control the movement of a cursor [Wolpaw *et al.* (1991) & Kubler (1999)] or other external device [Millan *et al.* (2004)]. However, in addition to being contaminated by noise sources such as eye blinks and facial movements, the EEG signal becomes highly attenuated by the skull and surrounding tissue making on-line decoding of surface detected EEG a complex problem. For examples of such techniques see [Sykacek *et al.* (2004), Nicolaou and Nasuto (2003), James and Gibson (2003), Penny *et al.* (2000) & Jung *et al.* (2000)]. Issues are further compounded since scalp electrodes are notoriously difficult to accurately position and attach [Pfurtscheller *et al.* (2003)].

3.2.5.1 BCIs for Identification

Although clearly still in its infancy, non-invasive BCI technology has been highlighted as having several potential applications both in terms of digital identity, and specifically in AmI environments. For example, although fingerprinting has been hailed as a unique way to identify a person, the axiom on which this is based has more recently come under more detailed scientific scrutiny. The discovery that the individuality of fingerprints is questionable [Pankanti *et al.* (2000)] has prompted further research into novel biometric systems for identification (see FIDIS D6.1 for more information on current biometric techniques). EEG has to date produced convincing results [Ravi *et al.* (2005)], which suggest that an individual is actually uniquely identifiable using brain patterns, with an accuracy of up to 96.6%, a figure which actually rivals some other more established biometric systems.

Such research capitalises on the innate behaviour of the brain when presented with visual images that have previously been seen, or are being consciously sought after, i.e. the brain produces a unique signature of activity in the sub-conscious when an image is recognised. The appeal of this technique for identification is that is would be hard to replicate, i.e. forge, this biometric. However, other researchers have indicated the possibility of broadening the scope of such technology to allow the characteristics of any thought process to be uniquely identified. This has several advantages over 'classic' biometrics in that the user is able to change the thought (known as a 'pass-thought' [Thorpe *et al.* 2005]) in the same way that a password or PIN could be changed, as opposed to biometrics such as fingerprints which cannot be easily modified. Additionally, the available entropy (i.e. set of possible inputs) is notably large since such a thought could be anything from a simple word from any language, to a personal memory.

The existing solutions to actually detect the raw brain activity are still cumbersome, however, remote brain-activity sensors are becoming a reality. Optical sensors for example which use light to infer neural activity near the outer layers of the cortex by measuring reflection changes due to changes in blood-oxygenation levels have been developed. Such a device does not physically make contact with the head.

Security & Privacy

With any emerging security technology, one question is paramount: '*How reliable is it?*' Two technical issues exist that can be used to quantify an answer, that of a *false positive*, i.e.

concluding that someone is wrongly identified as an enrolled user of the system, and *false negative*, i.e. being unable to confirm the identity of a valid user. Whether BCIs are ultimately able to provide the correct trade off between correct and incorrect identification remains to be seen. However this technology has clear advantages when it come to the two most pertinent security issues relating to biometrics: the lack of secrecy of biometric data (for example, fingerprints are routinely left on objects during everyday activities) and non-replacability (i.e. once a fingerprint has been compromised it cannot be changed). Additionally whereas typical biometrics also suffer from *failure to enrol* i.e. fingerprints may be worn out or digits missing, it is thought that such techniques would not be as susceptible.

Beyond the inherent error-prone nature of biometric technology, there is the real possibility of deliberate attack in an attempt to compromise security. There are essentially a series of vulnerabilities of any biometric system regardless of the type of biometric being utilised.

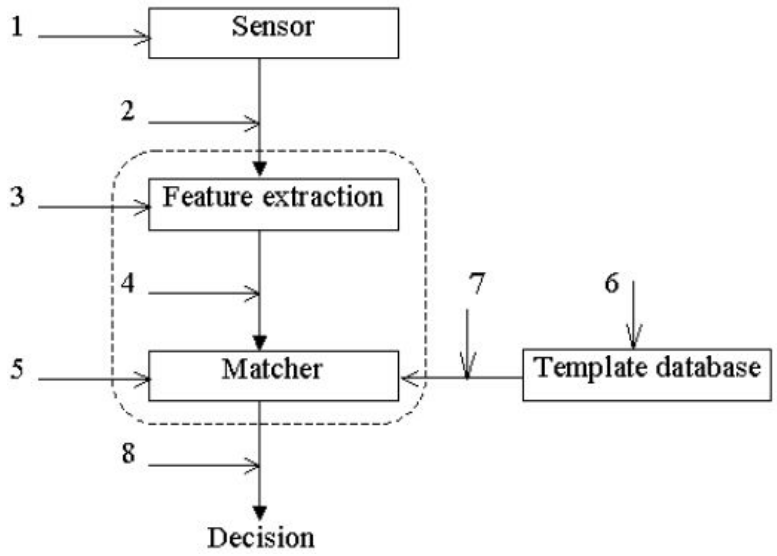

Figure 2: A block diagram of a generic biometrics system, with eight potential attack points highlighted. Adapted from [Uludag *et al.* 2004]

Figure 2 highlights the significant eight points within a biometric system which are open for potential attack [Uludag *et al.* (2004)]. The extent to which these can be exploited has a direct relation to the overall security of the system (see FIDIS D3.2 for more detail). The eight points of attack are:

1. Utilising an imitation biometric.
2. Although more complex, *replaying* previously submitted biometric data to cause a false positive identification.
3. By attacking the system at the feature module point, it is possible, albeit unlikely, for an attacker to force the system to produce values unrelated to the sensor input that subsequently generates a false positive result.
4. Replacing the system generated feature values with known valid ones will result in unauthorised access.

5. If the matcher can be forced into generating an incorrectly high matching score, then a false positive will result.
6. The template matching component is particularly vulnerable since incorrect data stored here (through error, collusion or attack) is open to abuse at any time. Data may be added, edited, removed or replaced so that an invalid user is authenticated. Database security is the key here to reducing vulnerability since unsecured templates can be reverse-engineered and synthetic data added.
7. By intercepting the transmission of the template data, and replacing the original templates with false data, a false positive can be generated.
8. By attacking at the decision end of the system, the binary result '*Yes / No*' can be modified to falsify the result.

Attack (1) is perhaps the most intuitive, yet minimised through the use of BCI based biometrics. The remaining attack techniques require a more intimate understanding of the specific authentication system and typically some degree of access to its inner workings. However, all component parts of the authentication system represent a potentially exploitable issue.

The ethical questions regarding such 'mind-reading' technology are clear, although currently the length to which this is exploitable is still scientifically unproven.

3.2.5.2 BCIs for profiling

In order to create a comprehensive profile of an individual, it is necessary to gain as much information as possible regarding their interactions, thoughts and feelings. If you can metaphorically "get into someone's head", then you have 'insider' knowledge as to the individual's feelings, reactions and emotional state. Whilst the concept of observing someone's thoughts like one can watch a television is intriguing, the scientific evidence currently does not support its feasibility. However, the fact that bodily responses are under neural control suggests that they may be able to provide windows into underlying psychological processes. For this reason there is great interest in the use of non-invasive BCIs for affective computing (see section 3.2.3).

A new field of research termed Augmented Cognition has emerged over the last few years, where the basic premise is to address cognitive bottlenecks (e.g. limitations in attention, memory, learning, comprehension, and decision making) via technologies that assess the user's cognitive status in real time. A computational interaction employing such novel system concepts monitors the state of the user, through behavioural, psycho-physiological and/or neurophysiological data acquired from the user in real time, and then adapts or augments the computational interface to significantly improve their performance on the task at hand [Schmorrow *et al.* (2004)]. In essence, such systems tend to reduce the amount of information the user is being exposed to, if indications reveal that the user is being overloaded. Unsurprisingly the applications in question are typically military related, i.e. reducing screen information to essential material if a pilot is becoming stressed. However, the advantages are that the technology being developed is designed to be robust and unobtrusive (in theory), and has clear application in AmI environments.

3.2.6 ICT Implants

While the field of Information and Communication Technologies (ICT) has expanded significantly over the past few years, few areas have created as much controversy as that of ICT implants. The recent developments in basic engineering technologies have meant that the integration of silicon with biology has already become a reality, and has prompted much research into the ethics of these technologies (see e.g. [EGE (2005)]).

Medical devices

Part of the drive behind the development of ICT implant devices is medical – i.e. restoring lost human abilities. Whilst society in general has come to accept artificial mechanical body parts such as artificial hips and heart valves, debate now rages about technologies based around computer technology. There is a fair range of such 'restorative' devices already in clinical use, the pacemaker being one of the better known. However, of greater interest is the development of technologies which are able to interact with us on a neural level. The most ubiquitous sensory neural prostheses is by far the cochlea implant [Zeng (2004)]. Where destruction of cochlear hair cells and the related degeneration of auditory nerve fibres has resulted in sensorineural hearing loss [McCabe (1979)], the prostheses is designed to elicit patterns of nerve activity via a linear array of electrodes implanted in the deaf patient's cochlea that mimics those of a normal ear for a range of frequencies. Current devices enable around 20 percent of those implanted to communicate without lip reading and the vast majority to communicate fluently when the sound is combined with lip reading. Its modest success is related to the ratio of stimulation channels to active sensor channels in a fully functional ear, with recent devices having up to 24 channels, while the human ear utilises upwards of 30,000 fibres on the auditory nerve.

With the limitations of the cochlea implant in mind, the retinal implant [Rizzo *et al.* (2001)] is certainly substantially more ambitious. While degenerative processes such as retinitis pigmentosa selectively affect the photodetectors of the retina, the fibres of the optic nerve remain functional, so with direct stimulation of the nerve it has been possible for the recipient to perceive simple shapes and letters [Liu *et al.* (2003)]. However, the difficulties with restoring full sight are several orders of magnitude greater than those of the cochlear implant simply because the retina contains millions of photodetectors that need to be artificially replicated. An alternative methodology is to bypass the optic nerve altogether and use cortical surface or intracortical stimulation to generate phosphenes [Dobelle (2000)]. However, progress in this area has been hampered by our lack of understanding of brain functionality, so to date has produced results no better than systems which simply utilise other functioning sensory receptors [Meijer (1992)] and thus potentially capitalise on cross-modal neural plasticity [Shimojo and Shams (2001) & Cohen *et al.* (1997)].

Electrical stimulation of the CNS has also proved useful in the treatment of other medical conditions. Earlier work by Delgado to artificially induce schizophrenia has subsequently been brought into question; however, more recently direct stimulation of areas within the brain has proven successful in treating the tremor, rigidity and bradykinesia symptoms of Parkinson's disease by manipulating basal ganglia activity [Gasson *et al.* (2005b)]. Work on rats [Talwar *et al.* (2002)] has also demonstrated how direct brain stimulation can be used to guide them through a maze problem, essentially by reinforcement, by evoking stimuli to the cortical whisker areas to suggest the presence of an object, and stimulation of the medial

forebrain bundle (thought to be responsible for both the sense of motivation and the sense of reward) when the rat moves accordingly.

The ability of electrical neural stimulation to drive behaviour and modify brain function without the recipient's cognitive intervention is clear, however, it can also be used to replace the natural percept, for example the work by Romo *et al.* [Romo *et al.* (2000)], demonstrating that local electrical microstimulation of the somatic sensory cortex can substitute for skin vibration in perceptual tasks that require frequency discrimination.

In the devices discussed above, the interaction is directly from the device to the human, i.e. information is *internalised*. To fulfil the requirements of seamless interaction, dataflow needs to be bi-directional and thus *externalising* technologies are required. The invasive alternative to surface EEG recordings (see section 3.2.5) is to record neural activity from the cortex by either placing electrodes inside the skull [Kennedy *et al.* (2004)] or by implanting electrodes into the brain, see [Donoghue (2002)] for a review. This invasive procedure has already given interesting insights into the neurophysiological functionality of the brain, with work on rats and primates [Chapin (1999) & Wessberg (2000)], supporting the hypothesis that the direction and speed of an *intended* movement is predicted in the motor cortex by the activity of populations of neurons.

Discussion

In the short term, the use of medical ICT implants raises several identity related security and privacy concerns. Although in the most part existing applications involve a uni-directional connection with the nervous system, the devices themselves are often capable of bi-directional communication with the outside world. This communication is typically via some wireless means to avoid the infection risks associated with percutaneous connections. By remotely accessing an implanted device it is usually possible to control the device, adjust its settings, read back stored data, and in some cases even gain access to 'live' biological information. An example of this is the more established pacemaker technology whereby data is logged internally for subsequent patient management which relates to the performance of the heart, activity of the device and so on. Access to the data is obviously vulnerable to typical attack methodologies.

More long term, the technologies discussed above may prove to be the basis of future commercial technologies which allow us improved interaction in more AmI related environments. The ability to form direct bi-directional links with the human brain certainly opens up the potential for many new application areas. Scientists predict that within the next twenty years neural interfaces will be designed that will not only increase the dynamic range of senses, but will also enhance memory and enable "cyberthink" - invisible communication with others and technology [Gee (2004)]. Already the foundations of this are being investigated, with direct nervous system to nervous system, augmented sensory function, and 'internet ready' implants being demonstrated (see e.g. [Gasson *et al.* (2005), Warwick *et al.* (2003, 2004a, 2004b, 2005)]).

Non-medical application

In less invasive procedures, human implantation of RFID devices has also been proposed for a variety of applications. In 1998, Professor Kevin Warwick of the Department of Cybernetics

at the University of Reading, UK became one of the first people to have such a device implanted. By being able to track and uniquely identify him, the departmental building was able to build a profile of his behaviour, and customise it to his preferences, including adjusting light levels, starting his computer, and even brewing the coffee on his arrival.

Figure 3: Prof. Kevin Warwick has a 2cm long identifying implant (shown enlarged, right) surgically inserted into his arm

In other applications, some four years later, implanted identifying tags have been commercialised to essentially replace 'medic alert' bracelets and to relay medical details when linked with an online medical database[9]. Other implanted devices have been used to allow the individual access to secure areas, and even to identify clubbers such that payment for drinks can be automatically debited from their account[10].

3.2.7 Nanotechnology

Currently, there is no common understanding of the term nanotechnologies. Depending on the scientific discipline such as physics, chemistry, computer sciences, machine building etc. different concepts and technologies are summarised under this term. They all have in common that very small structures, originally of the size below 1 µm (1 µm is 10^{-6} m) down to 100 nm (1 nm is 10^{-9} m) are used. In information and communication technologies (ICT) today structures smaller than 100 nm are already implemented. For comparison: the visible light has wavelengths from 400 to 700 nm.

[9] http://news.bbc.co.uk/2/hi/health/1981026.stm

[10] http://news.bbc.co.uk/2/hi/technology/3697940.stm

The term "nanotechnology" was introduced in science by Richard P. Feynman[11], physicist at the Los Alamos National Laboratory and later professor at the California Institute of Technology (Caltech), in a talk titled "There's Plenty of Room at the Bottom"[12] in 1959.

Today nanotechnologies have found a number of applications [Paschen *et al.* (2004), Hoffknecht, Teichert (2006)]:

- In chemistry e.g. as carrier for catalysts, paints with active surfaces to prevent dirt, colours for liquid crystal displays (LCD), thermal and chemical protection of surfaces or aggregate for tyres.
- In energy production, conversion and transportation e.g. as components for fuel cells, photocells and batteries, or for superconductive wires.
- In physics e.g. for sensors and actuators.
- In pharmacy e.g. as adsorbents for active pharmaceutical ingredients.
- In ICT e.g. for electronic components (such as transistors), integrated circuits (ICs) and micro processors

Development of microprocessors is of relevance in the context of identity and identity management, as it is one of the main driving factors for Moore's law[13]. In 1965 Gordon E. Moore observed that the number of ICs per square inch is growing exponentially over time; today a prediction of growth by factor 2 every 18 months is largely accepted. This growth in integration and density of ICs also courses a significant growth in processing power of micro processors. Since 2005 transistors of the size of 65 nm in micro processors are state of the art[14], memory chips[15] and micro processors[16] using 45 nm technologies are being developed.

This development has a large influence on data processing in general, including personal data. Indirectly also all types of Identity Management Systems (IMS) will take benefit from the resulting increased computing power and memory as more and more complex identity management operations can be carried out in shorter time. For example in the context of user controlled IMS (type 3 IMS) relatively complex cryptographic calculations of e.g. digital anonymous credentials are possible on smaller and smaller devices such as hand held computers or PDAs. In addition ICs are enablers for Ubiquitous Computing and they may also play an important role in solutions for energy supply of objects in ambient intelligent environments.

[11] See http://en.wikipedia.org/wiki/Feynman

[12] See http://www.zyvex.com/nanotech/feynman.html

[13] See http://en.wikipedia.org/wiki/Moore's_law

[14] See e.g. http://www.intel.com/technology/silicon/65nm_technology.htm and references cited therein

[15] See e.g. http://www.golem.de/0601/42943.html

[16] See e.g. http://www.intel.com/pressroom/archive/releases/20060125comp.htm

Research in nanotechnologies is being funded by many national institutions[17] and the EU.[18]

3.2.8 Sensors which detect Sensors

As already mentioned in the introduction one of the most challenging problems regarding privacy in AmI spaces is the question of control of the data collected by sensors. The existence of this data is an essential and necessary part of AmI and can not be avoided without losing much of the 'intelligent' behaviour of AmI.

The solutions proposed so far of usage of user centric identity management systems are only the second step. This kind of user controlled release of personal data only becomes meaningful if the direct (i.e. uncontrolled) ways of accessing that information are impossible or at least exorbitant costly. But this is not the case with AmI as it is envisaged today, where a huge amount of fixed sensors are distributed in the AmI environment. These sensors could be used to collect all kinds of personal data of a given person without even informing them that the sensors exist at all.

This leads to the general problem that despite the presence of laws which forbid the unauthorised collection of personal data by means of sensors, they would very likely have little influence in practice, when their violation is not even (in theory) detectable. Different solutions are proposed to cope with this problem - besides the trivial solution to accept the privacy and data protection problems in favour of the benefits offered by sophisticated AmI spaces. All of them are in an early (research) stage of development and could be understood as emerging technologies. They all need support by policy makers (resp. the society at large) and appropriate regulations, which define the general direction of acceptable solutions for the society.

One possible route to give the control of personal data back to the effected individual would involve the development of sensors which are able to *detect* (the existence) of sensors. These detectors should ideally be mobile so that each interested person can carry them with them. Notwithstanding the existence of rules which regulate the deployment and usage of sensors in AmI spaces, this gives every person at least the option to make an informed decision regarding their presence in certain environments.

But also detectors which are not mobile (in the sense that one can easily carry them everyday) are useful, if rules and regulations forbid the uncontrolled usage of sensors in AmI spaces. The very existence of these detectors can then be used as deterrence in order to prevent the illegal deployment of sensors - assuming that the related penalties are effective.

In general techniques for detecting sensors could be classified in different categories according to the 'part' of the sensor they in fact can detect. Possible categories are:

- **Detection of the sensor device itself** (or more precisely the process of collecting sensor data). This is principally feasible as long as the sensors are 'active' in the sense that they emit some signal (e.g. electromagnetic waves, ultrasonic waves, light etc.), which could be intercepted by the detector. Clearly it is much harder to detect 'passive sensors', which

[17] For example by the German Federal Ministry for education and Research (BMBF), see http://www.bmbf.de/de/nanotechnologie.php

[18] See http://cordis.europa.eu/nanotechnology/actionplan.htm

just receive signals without emitting any. Prominent examples are optical sensors and (passive auto-focus or fixed focus) cameras. However, such devices could theoretically be detected, if the 'processing' of the signal it detects leads to the some form of other emission. This could be for instance the release of electromagnetic waves as a side effect of an amplifier which is used in pre-processing the signal. It could also be detected through a variance of the electromagnetic field surrounding the sensor. Generally the detection of passive sensors is highly related to the area of active probing.

- **Detection of the transmission of the collected data.** In order to use the collected data for profiling in AmI space, the data has to be transmitted from the sensor to the processing unit. This is especially possible if radio transmission is used for communication - which makes sense if the sensors need to be deployed within existing buildings without the need to lay new cables for them. But even wired transmission of sensor data could be detected - even though the necessary effort is much higher. A supporting fact is that in AmI scenarios very often the collected data needs to be processed (and thus transmitted) as soon as it is available. This increases the chance of detection compared to scenarios where the collected sensor data can be stored temporarily and only transmitted once a day or a week.
  An interesting questions is how "bad" sensors could be detected, if the "good" sensors will sent all the time (e.g. if they utilise so called "dummy traffic"—a common privacy enhancing-method to hide if and when a sensor has to transmit some real data). In general the "bad" sensors could hide their traffic into the "noise" that all the other sensors produce. But on the other side it would be sufficient if a detecting device can investigate the number of available sensors (e.g. because of (sender) addresses use within the data transmission stream).
- **Detection of the power supply.** Most sensors need some kind of energy to work properly. Often this energy is provided by means of some kind of power supply. Assuming that in AmI spaces a huge amount of sensors need to be deployed making it impossible to lay a power cable to all these destinations one can deduce that the (local) power supply of a sensor will have only limited capacity making energy a valuable resource which should be used sparingly. Hence power save mechanisms like pulsed power supplies will most likely be used which could be detected using radio receivers[19].

The most common devices able to detect sensors are so called *bug detectors*. A *bug* - also known as *covert listening device* - is usually a combination of a miniature radio transmitter with a microphone. Most bug detectors in fact do not detect the bug itself but the radio transmission (as described above).

Bug detectors are available on the market in many different types (see Figure 4) and have been under active development for a long time. However, despite this their effectiveness is quite questionable.

[19] One can easily test this by placing a medium wave receiver nearby a TV operating in stand-by mode.

Figure 4: Different types of Bug Detectors for different purposes

Not much is known about available detectors for other kinds of sensors. A reason for this could be that such development is not within the scope of industry and academic researchers. Another possible explanation is that the strong natural interests of law enforcement and intelligence agencies to keep the information about sensors which could detect other sensors secret leads to missing literature about them. The latter is a general problem which might indicate a need for new laws or regulations regarding the availability of such detectors for private persons. Once again there exists conflict between the interests of law enforcement agencies performing surveillance and the data protection interests of citizens in counter surveillance.

But even if one assumes that the usage of sensor detectors is lawful, it can be anticipated that for certain areas of application[20] a race between sensor and sensor detector manufactures will take place. From an electro technical point of view - given our current knowledge - one can assume that the detection of well designed sensors will always be a hard task - if not impossible. This means that, in the long run, the sensor manufactures might win the race. Therefore besides sensor detectors, other possible technologies need to be discussed in order to solve the privacy problem within AmI spaces, as mentioned above.

One possibility is to perturb the effectiveness of the sensors. A well known approach is to emit jamming signals which can either influence the sensing device directly or could try to disrupt the (wireless) communication of the sensor. The latter is known as radio jamming.

In general it seems to be easier to disturb sensors than to actually detect them. Nevertheless it is still a challenging task, especially if the jamming device has to be mobile so that everyone can carry it with them. Moreover it again becomes a question regarding laws and regulations, because the emission of jamming signals in a given AmI space may also influence the effectives of the sensors regarding other people (and therefore the quality of service which could be offered to them). Hence it seems to be necessary to hold a general decision regarding whether sensors deployed in AmI space are allowed and whether jamming them or not shall

[20] E.g. if an operator of a given AmI space believes that he will get a competitive advantage if he violates the privacy laws (because there are usually only small sanctions). Given how some companies act today this does not seem to be unlikely.

consequently be allowed or prohibited. Taking this decision is even more necessary, if it comes to a more irreversible disturbance of sensors, i.e. their destruction.

In the case where it is decided to allow the deployment of huge amounts of undetectable sensors within AmI spaces, the laws and regulations shall be adapted in order to demand that every lawful sensor emits information about itself in a machine-readable manner. These data (following the privacy law principles) shall at least include information about the location of the sensor, its purpose and capabilities and information about who will process the collected data, for what reason (the data controller) etc. The regulations of today, which only require the placement of a sign somewhere in the environment (e.g. in case of video surveillance), is far behind the needs arising in AmI spaces. Although simple signs are not useful for all people (e.g. they can not be read by blind people), the vast amount of sensor-related signs will overload the perceptional capabilities of human beings. Therefore one needs some informational condensing, which can be realised via a personal device, which runs a similar identity management system, as to that described in D7.3. This device can create warnings based on the measured and calculated privacy risk implied by the environment and the preferences regarding privacy and protection of personal data of the user.

3.2.9 Mobile sensors for AmI

The question may arise as to why one should trust that an operator of a given AmI space will not deploy 'unmarked'(i.e. hidden / undetectable) sensors, whereas at the same time one may not trust that the operator will not misuse the collected data (this is why PET technologies are used at all). Possible answers might be that it is always more difficult to detect things which happen in cyberspace than detecting the existence of physical objects or indeed imposing penalties for the deployment of forbidden sensors may prevent their use. Furthermore in an AmI space a service provider might not even have the full control over who is processing the collected data, for which purpose etc., but he might more easily control which sensors are deployed in his facility.

Being aware of all the privacy problems arising from fixed sensors deployed in AmI environments one could question this concept as a whole. Although at the moment a frontier research area, one can speculate that mobile sensors may be a future emerging technology for AmI. The central idea is that instead of embedding sensors and computing devices into the fixed environment (floors, walls, streets, pedestrian zones, ...) or semi-fixed environment (cars, railways, ...), sensors and their directly attached evaluation by computing are embedded in our mobile environment (clothes, shoes, glasses, wrist-watches, mobile phones, pens, ...). Then, the communication between humans with their fixed or semi-fixed environment can exclusively (or at least mainly) be by means of their mobile environment using a digital (wireless) interface to the fixed or semi-fixed environment. This digital interface gives individuals a much more reasonable degree of control over which personal information is communicated and therefore is known (potentially forever) within the fixed or semi-fixed environment. This application scenario largely assumes that sensors in the fixed and semi-fixed environment are banned and/or jammed by the mobile environment and their functioning including the computing of their signals is closely regulated and monitored. Computation of personalised filtering and interpretation by the mobile devices enables a change in the main direction of information flow from (semi-)fixed environments to the individual instead of vice-versa. This change of direction enables a quantum leap in privacy by avoiding creating possibilities to gather huge amounts of personal data. As a special case

of this reversed information flow, the environment could give all kinds of safety and security advice (including advices for privacy) to the individual.

Summarising one can say that deploying huge amounts of sensors would lead to a massive loss of control over personal data. All users should be informed about this and the alternative possibilities, in order to make sure that any decisions made are based on the correct information. In any case the regulations should be changed in a way that obliges operators of sensors to communicate information about the sensors in a machine-readable and easy to access way and provide for fines, in cases of breach of this obligation.

3.3 Supporting Emerging Technologies for AmI

3.3.1 Energy Supplies

One of the basic requirements for ambient intelligence or ubiquitous computing support is the availability of electric energy for objects in the environments. How can these embedded and partially mobile sensors, actuators or micro processors be supplied with electric energy? Certainly cabling them in a traditional way is not an acceptable solution; costs will be very high and mobility of cabled devices is limited. In this context two approaches are of importance [Bizer *et al*. (2006: 65)]:

- Reducing the energy consumption of these devices so that traditional sources of energy can be used over a longer period.
- Finding new or more efficient ways for energy supply of these devices

The first approach can be achieved by more integrated and efficient micro processors (section 3.2.7) and more efficient programming. In addition to more efficiency in internal code, the use of more efficient wireless communication and routing protocols is an important task in reduction of energy consumption [Bizer *et al*. (2006: 66)].

In the context of new and more efficient ways for energy supply, the following approaches seem to be very important:

- Improved rechargeable batteries based on a higher energy density compared to today's solutions: this could prolong recharge cycles for mobile and fixed components.
- "Energy Harvesting" [Satyanarayanan (2005)]: using motion, differences in temperature or sound waves energy can be extracted from the environment and used for energy supply mainly of mobile devices.
- Fuel cells[21]: using different type of fuel such as hydrogen, methanol or methane, the chemical energy of the fuel is directly concerted into electric energy with an efficiency of up to 70%.

[21] See http://de.wikipedia.org/wiki/Brennstoffzelle

Hydrogen is not a primary energy carrier, i.e. it is not a natural energy resource and needs to be synthesised from water using electric energy. In this context methanol receives more attention as a renewable and natural energy resource. Different prototypes of methanol fuel cells as energy sources for notebooks are already available. But energy efficiency is still a problem, as only 50% efficiency seems to be achievable today for this type of fuel cell. As a consequence heat from the fuel cells, for integrated systems such as a notebook, is still a problem. In addition these types of fuel cells are still quite heavy (around 1.7 kg).[22] It can be expected that with the development of improved membrane materials for fuel cells energy density and efficiency can be improved significantly in near future.

New and more efficient ways of energy supply for ICT are a basic technology for AmI and thus indirectly influence identity management in ambient intelligent environments. In European Member States in general, research in energy supply in the public sector seems mainly to be focused on renewable energies and improving energy efficiency. Such research for systems and devices in AmI environments currently seems to be driven mainly by private organisations (see examples in this chapter).

3.3.2 Smart Materials

According to a definition given by McCloskey (2004) smart materials are "non-living material systems that achieve adaptive behaviour". Examples of smart materials are compound materials using piezo-electric fibres or polymers that are electrically or magnetically active. Other examples are shape memory alloys (SMA), i.e. metals that after being deformed return back to their original shape when heated. Micro-electro-mechanic systems (MEMS) are also understood as smart materials. They are combinations of e.g. sensors or actuators or other electric circuits integrated on a computer chip. MEMS are used, for example, in the wings of aircrafts to detect and measure the degree of deformation.

Smart materials may play a major role in the context of new sensors and actuators in AmI. Actuators and data from these sensors may be subject to identity management in ambient intelligent environments.

Public research institutions seem to play a major role in research in smart materials as well in Europe[23] as the USA[24]. The European Union actively supports projects in the context of smart materials.[25]

3.3.3 Networking & Communication

The levels of interaction that may occur between the user and the technology within the AmI context is shown in the "MultiSphere Reference Model" (Figure 5).

---

[22] See for example http://www.heise.de/newsticker/meldung/70168

[23] See for example die Fraunhofer Gesellschaft in Germany: http://www.smart-materials.fhg.de/

[24] See for example http://www.cs.ualberta.ca/~database/MEMS/sma_mems/smrt.html

[25] See for example Projekt PolyApply (The Application of Polymer Electronics to Ambient Intelligence): http://www.polyapply.org/

Figure 5: A visualisation of the MultiSphere Reference Model [WWRF (2001)] showing various layers of interaction desirable in the AmI scenario

Although this model aims primarily at putting issues and ideas of wireless communications in context, from such models the following interaction levels can be identified [Riva (2001)]:

- Body area network (BAN) connecting sensors, chips or devices attached to the body/clothes or implanted in the body (distance: <1 meter)
- Personal area network (PAN) consisting of personal and/or shared devices or peripherals (distance: <10 meters)
- Local area network (LAN) for the nomadic access to fixed and mobile networks, and to the Internet (distance: <100 meters)
- Wide area network (WAN) for the access and routing with full mobility (worldwide access)
- The 'Cyberworld' where users and intelligent agents interact (virtual)

To fulfil the current vision of AmI, it is necessary that fluid communication between these layers is realised through the use of interoperable hardware and software standards and protocols.

'Body-centric' wireless communications is a new and developing field which refers to human-self and human to human networking through the use of wearable and implantable sensors. Existing technologies which allow portable devices to connect are typically based on PAN standards such as 802.11x or on Bluetooth. Neither of these are spectrum efficient for

BANs in that most of the radio energy becomes directed away from the body when the radio antenna is placed close to the skin. As such BAN is an area where standards are only now starting to be defined.

3.3.4 Grid Computing

Building, providing and maintaining the infrastructure required to support the AmI environment will be an extremely difficult task. Both functional (related to the specific system operation) and non-functional (security, scalability, performance, robustness, availability, reliability, licence issues, etc) requirements of an AmI system pose strict demands on the computational and communication resources and in general on the underlying infrastructure. However, the promising results of the feverish research in the field of Grid Computing in combination with the on-going efforts of its wider adoption in industry and business indicate that the infrastructure required for AmI is actually on the way and, thus, the implementation of AmI systems with strong real-time, security or reliability requirements or large-scale AmI systems may not be that distant.

As grid computing is an emerging technology, many approaches to define it exist. In an effort to capture the different aspects of grid computing in one definition, Ian Foster [Foster *et al* (2002)] defines the Grid as a system that "*coordinates resources that are not subject to centralised control using standard, open, general-purpose protocols and interfaces to deliver nontrivial qualities of service*". This definition goes beyond defining the Grid as simply an infrastructure delivering the power of multiple computational resources to a single user-point for a specific application by uniting these resources (pools of storage systems, processing units and networks) into a single system. The Grid has thus no central administrative control but involves the integration and coordination of users and resources of different control domains based on standards, seamless and open protocols and interfaces dealing with issues such as, authentication, authorisation, service level agreement establishment, resource discovery, negotiation, reservation and service execution, for the delivery of various qualities of service, including requirements concerning response time, availability, throughput and security. According to Berman, Fox and Hey [Bergman *et al* (2003)] "*Grid infrastructure will provide us with the ability to dynamically link together resources as an ensemble to support the execution of large-scale, resource-intensive, and distributed applications*". Thus, the vision of the Grid is the provision of global – if possible - infrastructure for scientific, business, managerial, governmental and commercial purposes, as well as daily activities.

Initially the idea behind the Grid was the exploitation of idle computational cycles. Based on the observation that most computers remain idle for almost 90% of a typical day, the Grid was seen as the technological solution to the problem of the widely distributed unused computing capacity. Grid computing is regarded to be the future of Semantic Web[26], the next step in distributed networking. The Grid may include systems which are geographically dispersed, belonging to different organisations, running different operating systems on heterogeneous hardware platforms. The user, however, should be able to have uniform access to these resources; in other words, the Grid is presented as a single large virtual computer.

[26] Semantic Web is an extension of the World Wide Web in which web content cannot only be expressed in natural language, but also in a machine-processable way.

	Electrical Power Grid	**The Grid**
Transparency	No need to worry about how or where the electrical power you are using is generated.	No need to worry about what computer/s is used to process your request or where the data it requires is. The middleware is responsible for assigning the submitted task to the resource which is more suitable for performing it (in terms of availability, workload and the quality of service requested by the user, etc.) and will work the best possible way to locate and retrieve the data needed.
Pervasiveness	Electricity is widely accessible and accessing it requires only a standard wall socket.	No special requirements for accessing the Grid exist. Different platforms, such as desktop computers, laptops, PDAs and mobile phones, will be able to access the Grid resources simply through a web browser.
Any access point serves	At any socket the electrical appliance is connected to it will get the electricity it requires for operating.	Any computer connecting to the Grid will be served by it as if it were a local machine.
Utility	Electricity is provided as a service: you request for electricity and it is provided to you, and you are charged for what you use.	The Grid is envisaged to be a service which will simply provide resources based on the request. The charging will also be based on the use of the Grid and the quality of service requested.
Infrastructure	The underlying infrastructure is called "the power grid". It includes power stations, transmission stations and power-lines among others in order to link together different kinds of power plants with homes, factories, etc.	The infrastructure that is required for the provision of the above services is called "the Grid". It includes personal computers, servers, databases, networks, linked together.

Table 1: Electrical Power Grid and the Grid analogy

In general, the term infrastructure is used to describe a technology that lies under the application being used and the service provided and is taken for granted when these operations are performed. When making a phone call, the callers are not concerned with the switches, the repeaters and the general underlying network that connects the transmitter with the receiver. The Intern*et al*lows the communication among different, geographically dispersed devices. Similarly, the Grid must be able to provide on-demand access to computing, and thus be widely deployed. The latter, however, requires that the Grid infrastructure must be simple and provide more functionality than the underlying Internet at the same time.

Grid computing, as a term, was initially adopted in order to capture the vision of scientists and researchers to make computer power as easy to access as electricity through the electric power grid. Potentially it must involve every protocol and computer technology that already exists

with its scope thus being extremely wide. Table 1 summarises the similarities in the core idea and operation of the electrical power grid and the Grid [Chetty *et al.* (2002)].

3.3.4.1 Grid Classification

In an effort to classify the applications that will take advantage of the Grid by running on it, Allen *et al.* identified an initial list of categories of Grid applications with the classification criterion being the main driving reason for using the Grid [Allen *et al.* (2003)]. According to this classification scheme, the categories of Grid applications are the following:

- Community-centric

Such applications are used in a collaborative environment and thus involve and require various interactions among people or communities. Such a collaborative environment could be scientists and engineers cooperating to design and produce a new vehicle or a smart surveillance system processing input from various geographically dispersed cameras and microphones.

- Data-centric

These Grid applications require storage, management, mining and transfer of large amounts of data between distributed and/or heterogeneous databases. Examples of such applications include DNA analysis applications and weather monitoring based on processing of data received by sensors placed on various locations around the globe.

- Computation-centric

The applications in this category are the common computationally demanding applications, such as weather forecasting, climate modelling, world economy modelling, and earthquake simulation. For years the limitation of computational resources has been forcing scientists and engineers to intentionally omit important factors affecting these models so that these applications produce a result in reasonable time. This leads to a compromise in the precision and thus the reliability of the produced models.

- Interaction-centric

One of the strongest requirements of these applications is responsiveness due to real-time user interaction which in turn requires robust and effective real-time data processing and analysis. Examples of such applications include the submission of orders by customers and their processing and monitoring by suppliers and distributors in supply chain management and online gaming applications.

Having functionality as the classification criterion, the following categories of the Grid exist:

- The Computational Grid

It embodies the initial idea behind the Grid. Its main aim is to speed up the applications by sharing their processing needs to several computational resources (processing units, memory units, disks) and coordinating them.

- The Data/Information Grid

This type of Grid focuses on the controlled data access, sharing and management. The data may be heterogeneous, distributed and of large amount. A Data Grid offers great advantages to data-intensive applications including performance and security improvement.

- The Equipment Grid

It links together different types of equipment, including telescopes, cameras, microphones, health monitoring devices, and other sensors and devices.

- The Enterprise Grid

This type of Grid integrates all the above mentioned Grids. Every user of the Enterprise Grid is able to get from the Grid the resources his applications require any time he uses them as if his applications are being processed locally. It provides prompt access to available information and executes computationally demanding applications in a reasonable time requiring the least possible intervention of IT experts during the resource provision and system operation.

Another Grid classification based on the scale of the Grid divides the Grids into Cluster Grids, Enterprise Grids, Utility Computing and Community Grids. More specifically:

- Cluster Grids

The resources shared in Cluster Grids are physically located in the same place and are mainly used inside companies for resource coordination, workload balancing and backup mechanisms.

- Enterprise Grids

The resources are physically distributed within the company and the applications using them are operating behind the corporate firewall.

- Utility Computing

The resources are provided by a third party service provider who hosts and manages the Grid application and the Grid resources. These resources may be provided to more than one organisation, whereas the organisations are paying for their use based on the charging scheme which has been agreed between them and the service provider.

- Community or Partner Grids

This type of Grid involves the collaboration of various organisations which all share resources based on predefined agreements forming what is called a Virtual Organisation (VO), a term better described in section 3.3.4.4.

3.3.4.2 The Semantic Grid

The Semantic Grid is the projection of Semantic Web in the grid computing area. It is an effort to apply the main principles of Semantic Web to the Grid. The Semantic Grid was initiated by the need of having a description of the information in the Web so that it is more easily and efficiently discovered and retrieved. This need was not satisfied by HTML which is a mark-up language focusing on formatting and not tagging content. According to the

semantic grid group[27], the semantic grid is "an extension of the current grid in which information and services are given well-defined meaning, better enabling computers and people to work in cooperation". Similarly with the Semantic Web, the Semantic Grid includes a detailed description of the services and the resources in the Grid, which allows for a more efficient service and resource discovery. Moreover, grid resources and output of grid applications can be connected and integrated and useful and intelligent associations of data can be produced. Such an example could be searching texts for a word as well as audio files which contain this word.

3.3.4.3 The Mobile Grid

In an effort to address the issue of mobility, a requirement posed by many applications, and thus, leverage the large set of mobile users, research has also been focused on the Mobile Grid. The Grid, while providing services to the users, must be able to deal with issues of network handovers concerning both the users and the resources. Thus, it must be adaptable and able to dynamically configure the services, the resources, the network and the security. [Litke *et al.* (2004)] The Mobile Grid could be the extended grid infrastructure that could support the provision of location-based services. In the Mobile Grid, users can be mobile with their location changing often or rarely, leading to a need of instant knowledge of the user's new location and related context. The simplest example could be a user wanting to download a file. If his current location is much closer to a computer storing this file than the previous one, then the Grid should be able to adjust to the new context. In the case of a mobile resource, which could be either a computational resource or an expert (such as a doctor or a teacher), the Grid must be able to either update the system with the new location of the resources, so that access to that resources is still possible, or locate a new resource satisfying the user's requirements.

3.3.4.4 How Grid Computing works

As already mentioned, the Grid requires that resources are shared beyond the local administrative domain. These resources include disk storage, memory, processing units, data, peripherals, scientific instruments, software, licenses or even individuals (e.g., experts). This dynamic collection of institutions, individuals, software and computational resources forms a new administrative domain, which is called Virtual Organisation (VO). Each entity participating in the VO must clearly and carefully specify what it wants to share, who will be allowed to share, which the sharing conditions will be. Examples of VOs are: the suppliers, distributors, stock managers, application service providers, storage service providers working in the supply chain management on one hand; the simulation systems, the models, storage service providers, technicians, engineers, involved in aerospace engineering on the other hand. Both examples include VOs which are collaboration-demanding with the first one having mainly strong requirements in data management, security and user-friendliness and the second one being computationally and data demanding. As it is clearly seen in the examples above, the purpose, the size, the structure, the lifetime and the scope of VOs may vary. Nevertheless, a thorough technical analysis of their requirements forces the identification of

[27] http://www.semanticgrid.org/

common concerns and requirements addressed by a set of services which implement these common core functionalities [Foster *et al.*, (2001)]. These core functions of the Grid include execution management, data management, resource management and virtualisation, security and portals. In the following figure an example of an architecture integrating these core functionalities with a user (individual or application) accessing the Grid through the portal is depicted.

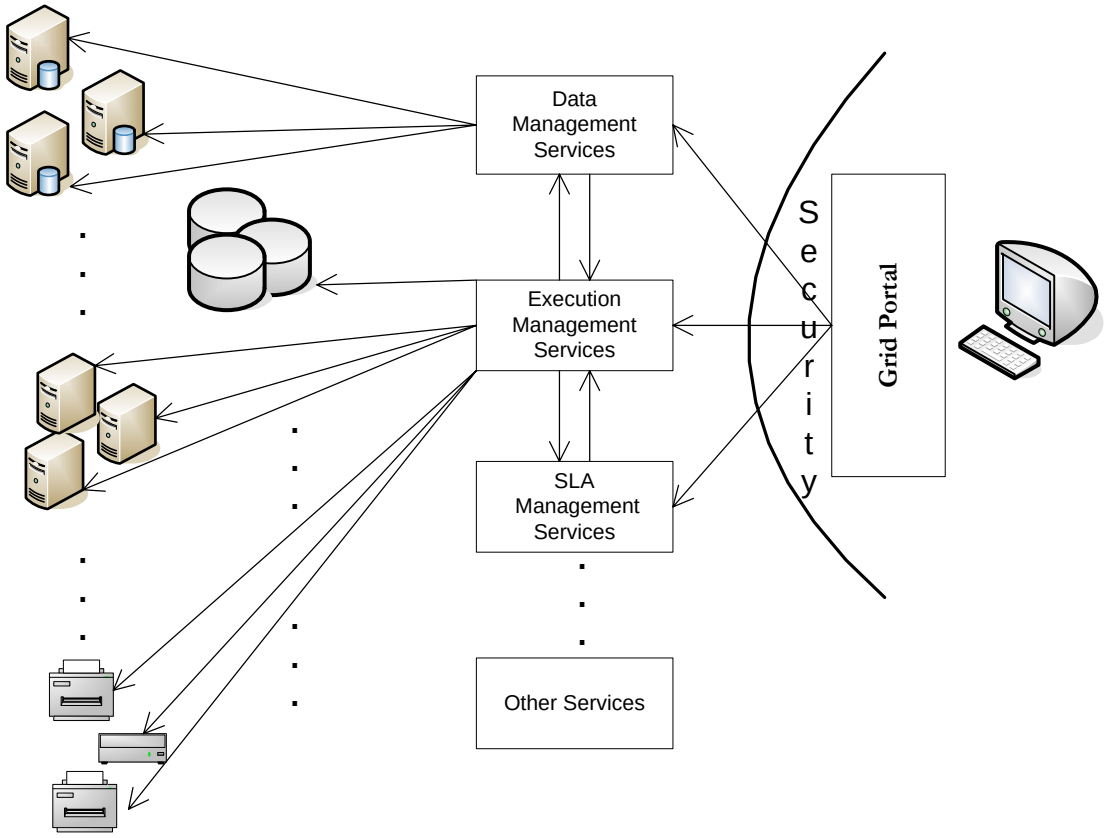

Figure 6: Example of a user accessing the Grid

In order for a user to be granted access to a grid resource, the service provider (SP) requires that a contract - the Service Level Agreement (SLA) - is firstly signed between the parties involved. The SLA should contain not only the legal description of the parties, but also offered and requested quality of service (QoS), technical and organisational security measures (Security Service Level Agreements, SSLAs), expected usage of the resources, SLA lifetime, compensations, penalties for not meeting service requirements, priority, as well as issues of pricing. In other words, the SLA specifies the terms of the agreement between the SP and the customer, including the charging of the services provided. Examples of the contents of the agreement include the amount of time the SP guarantees that the service will be up and running, the response time of the service, the mean time between failures of the service, the amount of time the service will require to be brought back up, the information rate. The SP publishes the services he can offer and the user-customer publishes the quality of service he wishes to be provided with. A cycle of negotiations takes place at this point with each of the

two sides aiming at making the contract as profitable as possible for themselves. As soon as the SLA has been agreed on, the SP must guarantee that during service provision the agreed-upon QoS is actually offered.

When the user wants to access the grid resources he has an SLA for, he accesses the Grid through an interface provided by the application he is running or an interface the grid administrator provides, the portal. The portal is a web interface that enables the user to submit jobs for execution on remote computing resources, monitor their execution by viewing job status, manage their execution by suspending, resuming or cancelling them, view job history, visualise the executed jobs (e.g., simulation results) and manage user accounts and their access rights. The term job in grid computing includes simple processes, such as a database query, or complicated processes such as simulation of a car crash or visualisation of a car virtually assembled by its various components.

Once the user submits the job in the Grid, the Execution Management Services (EMS) take action. According to OGSA, the Open Grid Services Architecture [Foster *et al.*, (2005)], developed by the Global Grid Forum (GGF), the EMS are responsible for finding candidate locations for the execution of the requested job, selecting the location based on different policies or service level agreements, preparing the environment at the selected location for the execution, initiating the execution of the job (e.g., registering the service to other services) and managing the execution of the job. Thus, after the job has been submitted by the user to the system, EMS perform resource discovery and reservation for the timeframe the user has requested. At this point issues such as priority, job queues and current allocation of resources (workload) determine the scheduling of the job. Ideally the system must be able to match peaks of some resources usage with lower usage of others so that the resources are being exploited in the best possible way and the jobs submitted are best-executed so that the user gets the impression that the job is being executed locally. After the resources that satisfy the SLA are found and are reserved, these resources are prepared – if necessary – (e.g., installation of a program on the machine the job is to be executed on) and then the job execution starts.

In general, while being processed, a submitted job may require the transfer of data, as well as the access to data from different locations, which may be heterogeneous and encounter various protocols. The Data Management Services are responsible for these operations. While the job is being executed, there is a chance that execution failure occurs due to a number of reasons, including network failure, program crash, data server going down. Thus, fault tolerance mechanisms need to be implemented. The action to be taken may be communicated by a Policy Manager Service, which stores and manages the policies. The Execution Management Services can reallocate resources and continue the execution of the job to the new resources or attempt to reallocate the initial resources. Moreover, the Data Management Services may offer data replication - multiple copies of the data (replicas) being maintained, which must be synchronised - so that in case of inability to access a database, a replica is being accessed and the execution of the job continues unobstructed. Furthermore, balancing of overly utilised storage with under-utilised storage improves the performance of the system.

There is a chance that an SLA violation occurs while the job is being executed, such as the time the service required for getting back up and running was more than the one in the SLA contract or more disk space was used. The system must then decide according to the Policy Manager Service and the agreed-upon SLA what actions it should take, such as stop the

execution of the job or charge the user for the extra resources (penalty) according to the charging scheme applied to the user.

As far as the charging of the grid usage is concerned, the SLA Management Service must have collected the data related to the consumption of the resources the metrics for which have been defined in the SLA by keeping accounting records. Various charging schemes can be applied. These can be based on the service usage or be fixed. Moreover, discounts for provision of lower quality of service as well as penalties in cases of SLA violation can be taken into account [Yeo and Buyya (2005)]. It should be noted, however, that the system is only responsible for maintaining the accounting records and applying the respective charging schemes, whereas real money transactions take place using the normal channels (credit card transactions, invoices in the mail, and other payment schemes).

3.3.4.5 Security Aspects of Grid Computing

As stated in the introduction, Grid Computing is one enabling technology for AmI spaces. A lot of sensor collected data will be processed for profiling using Grid Computing. Therefore it is important that the processing of this personal data happens in a secure and privacy preserving way.

As described in the technical section, one of the main visions of Grid computing is that the computing power of the Grid should be provided to its users in pretty much the same way as electrical power is provided by the power grid. Especially the user needs not to care about *who* is providing the resources. Therefore one can not assume that any kind of trust relationship between a Grid user and the Grid resources providers exist.

Hence a fundamental security issue is that the user of the Grid computing wants not only to protect the data which should be processed by the Grid resources against some outsiders (eavesdroppers on the network links etc.) but also against the administrators and owners of the Grid resources.

In general security is one part of the Open Grid Services Architecture (OGSA) [Foster *et al.*, 2005] as developed by the Open Grid Forum (OGF). But regarding the OGF documents and specifications one has to differentiate between *identified security requirements*, *offered security mechanisms according to the specifications* and *actually implemented features*. The latter is analysed using the Globus Toolkit[28] [Foster *et al*. (2006)] as reference implementation.

Most of the described security requirements, features and mechanisms are related to ***authentication*** and ***authorisation***. The most fundamental assumption is that each user and principal will have a Grid-wide identity that all the other Grid principals can verify [Humphrey *et al*. (2003)]. This means especially that the anonymous usage of Grid resources is not intended. For the use case of Grid computing within (classical) AmI spaces this is not a serious drawback, as the AmI space service provider is the user of the Grid - and not the person who enters a certain AmI environment.

[28] "The Globus® Toolkit is an open source software toolkit used for building grids. It is being developed by the Globus Alliance and many others all over the world. A growing number of projects and companies are using the Globus Toolkit to unlock the potential of grids for their cause". See http://www.globus.org/toolkit/

But it will become a problem for privacy enhanced AmI space if techniques like user centric identity management are used and the necessary processing of data is outsourced from the personal devices of the user to the Grid. In this case the user of the AmI space will also become the user of the Grid. Therefore all the profiling techniques described in the FIDIS deliverable D7.2 could harm the privacy and protection of personal data of the user. Hence the further development of the OGSA specifications should consider the anonymous and pseudonymous usage of Grid resources.

In [Humphrey *et al*. (2003)] different security related scenarios of Grid usage are illustrated. From these scenarios the OGSA security requirements for Grid computing are derived. Most of these scenarios deal with the problems of protecting the Grid resources (or the Grid at large) against malicious users (outsiders). Although it is an important prerequisite for achieving confidentiality and integrity of the processed data, it is not sufficient (as explained above).

The authors of [Humphrey *et al*. (2003)] are (to some extent) aware of this fact. Therefore they have specified that "[a]n individual Grid user should have the capability to constrain the manner in which she interacts with the collective Grid services." Implications of this requirement are:

- "Services must recognise the rationale for per-user security configuration and be designed accordingly.
- There must exist an easy mechanism for users to specify such constraints.
- There must be a secure and efficient mechanism to propagate or otherwise convey a particular user's integrity and confidentiality parameters from the user to the services."

In an extension to this [Humphrey *et al*. (2003)] identifies also that "a user may want to specify that certain files be encrypted or all the data at a given site be encrypted. The user may also wish to specifically mandate that a server that acts on her behalf store all data related to her encrypted."

Even though these requirements supporting the usage of the Grid in a privacy preserving manner they still miss some important points. First of all the confidentiality of the *processing* of the stored data is not covered. Secondly it remains unclear who can decrypt the encrypted data - only the Grid user or also the administrator of the Grid resource?

If it comes to the specifications of the actual architecture, then it turns out that the requirements mentioned above are not implemented rigorously. Besides authentication and authorisation - which constitutes the main part of the security specifications - only transport level security is considered. This will offer confidentiality against outsiders but not insiders.

Also the Grid Security Infrastructure (GSI) - which is the name of the portion of the Globus Toolkit that implements security functionality - will not achieve more than simple access control of Grid users to resources. In [4] an example is given how GSI will work for that purpose. Moreover the paper claimed that "[f]or simplicity many details of the security process, such as […] privacy are omitted. These functions would be implemented similarly, with the hosting environments using OGSA services to provide the needed functionality."

Unfortunately a 'simple' adoption of the mechanisms and techniques used for authentication and authorisation for achieving privacy and protection of personal data is not possible - especially if protection even against the providers of the resources is a requirement. Hence

even 'plain' confidentiality of the data processed within the Globus Grid is an open issue and only rudimentary solved by implementing (optional) transport level encryption.

Summing up one can state that secure and trustworthy computations with personal data without privacy risks are not possible using today's Grid architectures. It seems that protection against the operators of the Grid infrastructure and the various resources is not a big issue for the OGSA. Nevertheless solutions for that problem are thinkable by the means of cryptographic technologies like secure multiparty computation or the application of Trusted Computing.

Another open issue is the conflict between 'transparency' of the Grid i.e. that a Grid user need not (or even could not) know who is providing the resources, where the data is etc. and the requirements by law, when it comes to the processing of personal data.

In [Grimm *et al*. (2006)] it is illustrated using a medical research Grid application as an example. The patients taking part in the related research have to consent to the processing of the personal data - and they have the right to revoke this. This revocation requires that all data is deleted in a comprehensible and verifiable way. But this requires that one knows all the involved Grid resources - which fundamentally violates the transparency vision of the Grid. One needs secure logging and auditing to reproduce the spread of the personal data. Even though this is also relevant for OGSA (for accounting reasons) it is unclear how this logging could be done so that the logs or audit trails could not be manipulated.

The processing of personal data might not only imply problems from a user's point of view but also from the resource provider's one. The processing of personal data may impose additional duties to him, e.g. to verify that the affected user has given his consent.

One can conclude that the OGSA should be enhanced in a way that allows the formulation of policies which consider the *type* of the data processed by the Grid resources. This would allow a resource provider to express if he is willing (and able) to process personal data or not or could be used by a Grid user to inform a resource provider that he should handle certain data according to the rules for personal data.

Besides this one should rethink if the current data protection and privacy laws - made with centralised service providers in mind - are still appropriated for the case there the personal data is processed by a highly distributed system formed by hundreds of different organisations without any central control[29].

3.3.5 Peer-to-Peer network architectures

The overall goal of Peer-to-Peer (P2P) based systems[30] is to provide (share) resources (like computing power, bandwidth or storage) with a high level of quality of service in a **cost-efficient** way to (with) its participants. A fundamental principle of the P2P paradigm is *equality*.

[29] See: Prof. Dr. Alexander Roßnagel: "Datenschutz in einen informatisierten Alltag" [roughly translating to: Date protection in the ages of ubiquitous computing], Friedrich-Ebert-Stiftung, Berlin, http://library.fes.de/pdf-files/stabsabteilung/04548.pdf, 2007.

[30] The more general term *P2P based system* is used instead of the more specific ones like P2P network or P2P application because most of the described mechanisms and techniques are applicable to both layers.

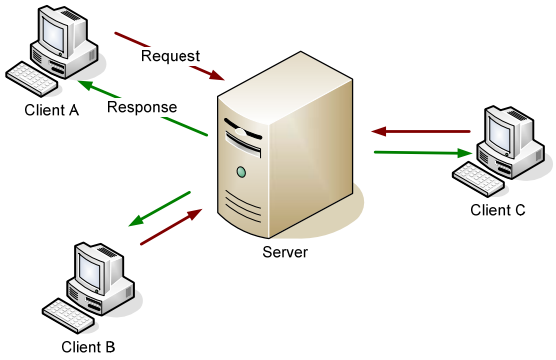

Figure 7: Client-Server based system

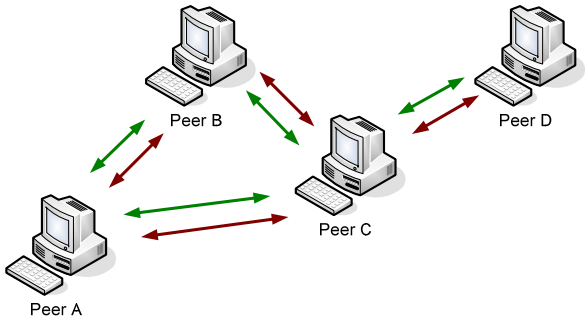

Figure 8: Peer-to-Peer based System

In classical client-server based systems (see Figure 7) a clear distinction of the roles and capabilities of the communicating entities could be made. Also a clear "direction" of the flow of information could be identified. One entity (which is called client) makes a request to another entity (which is called server). The server then processes the request and sends an appropriate response back to the client. Especially the clients never communicate directly with each other.

There are two fundamental problems with client-server based architectures centred on one server: scalability and robustness (availability). If the number of clients accessing a given server increases, then with nearly the same rate the resources of the server (in terms of processing power, storage and bandwidth) need to be increased to offer the same level of quality of service (e.g. in terms of latency) to its clients. This increase of server resources is connected with an (often non linear) increase of costs for the operator of the service. Also there may exist some 'physical' limitations, such as the maximum bandwidth the network connection could provide for a single server.

Therefore very often the server is not a single instance but in fact is a distributed system which implements some kind of load balancing among the nodes which forms the distributed server system. In this way the quality of service offered to the clients can be kept at a high level. Nevertheless the whole service infrastructure is still operated by the service provider and he bears the burden for all of the costs.

In a P2P based system (see Figure 8) every participant (also called node or peer) is simultaneously 'client' and 'server', meaning that it uses resources provided by others (acting as 'client') and offers resources to others (acting as 'server'). In this way the costs of operating / offering a given service are not anymore exclusively by the service provider - but shared among the participants. The service provider itself needs only to operate a small part of the infrastructure which forms the whole P2P based service.

P2P based systems in general offers a better scalability compared to client-server based systems. They are also more robust, meaning that unavailability of some nodes will not result in unavailability of the whole service. Because of the 'equality' paradigm other nodes of the system can take over the tasks of the crashed nodes. Or in other words: the existence of clients requesting a given service implies the existence of servers offering the requested service.

A P2P based system can be categorised by different properties:

- if it is a *pure* P2P based system or a *hybrid* system

- how the data transmission is organised: *single source download* or *multi source download*
- how information is found: *Centralised Directory Model (CDM)*, *Flooded Requests Model (FRM)* or *Document Routing Model (DRM)*[31]

A pure P2P based system strictly sticks to the 'equality' paradigm, i.e. all involved nodes are absolutely identical[32]. This kind of P2P based systems is the most robust system among the different types of P2P based systems. Such robustness also exists against unintentional failures of nodes (like crashes which let them disappear), as purposeful actions targeted for example to shutdown the whole network or to censor the available content.

In a hybrid P2P based system the 'equality' requirement is less stringent. In such systems one can distinguish different kinds of peers depending on the functionality they offer to the P2P network. The predefinition which node has to offer which kind of special functionality to the network could either be done statically (mostly at the time of deployment of the network) or dynamically (at the runtime of the network). In any case the proper work of the network depends on the existence of the special nodes.

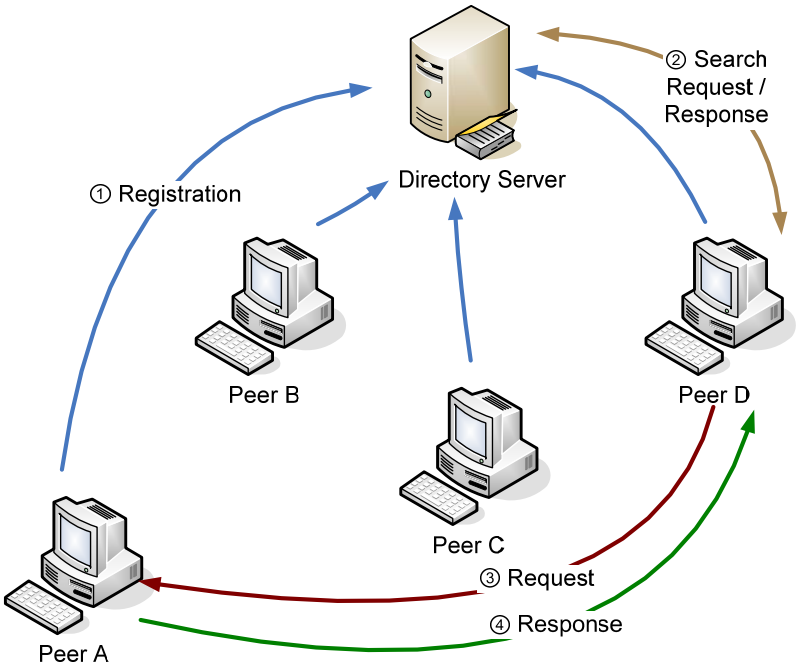

Figure 9: Hybrid P2P based system which uses the Centralised Directory Model for information retrieval

A typical example for a static hybrid P2P based system is a P2P network with some nodes dedicates as (centralised) directory server. The 'normal' peers register within the directory. If

[31] Other authors also use the terms *unstructured* resp. *structured* P2P network or categorise them according to be a *first*, *second* or *third generation* P2P based system. Notice that however it is named all essential techniques and mechanisms are described by the following.

[32] Here *identical* means identical from a conceptual point of view. Of course the physical instantiation of nodes can lead to some kind of inequality because the peers may use different hardware or software revisions.

a 'normal' peer needs a given resource (e.g. a file) it asks the directory for locations of that file. The file transfer itself then is done by direct interaction between the 'normal' peers.

The described mechanism of finding information is called Centralised Directory Model (see Figure 9). The well known file sharing service 'Napster' (in its original version) used this model. A disadvantage of the CDM is the limitation in scalability. Also privacy and data protection related problems arise. Because all search requests are managed by a centralised entity, this entity can build profiles of the peers, if no additional PET technologies are integrated into the P2P network.

Another property of CDM based P2P systems is related to controllability. The one who can control the centralised directory service can control which information is available to the 'normal' peers within the network. Depending on the application this could either be an advantage or a disadvantage of this type of P2P based systems. Also note that the very existence of the possibility of control may already burden liabilities (from a legal point of view) to the service operator. This was the case with the original Napster system.

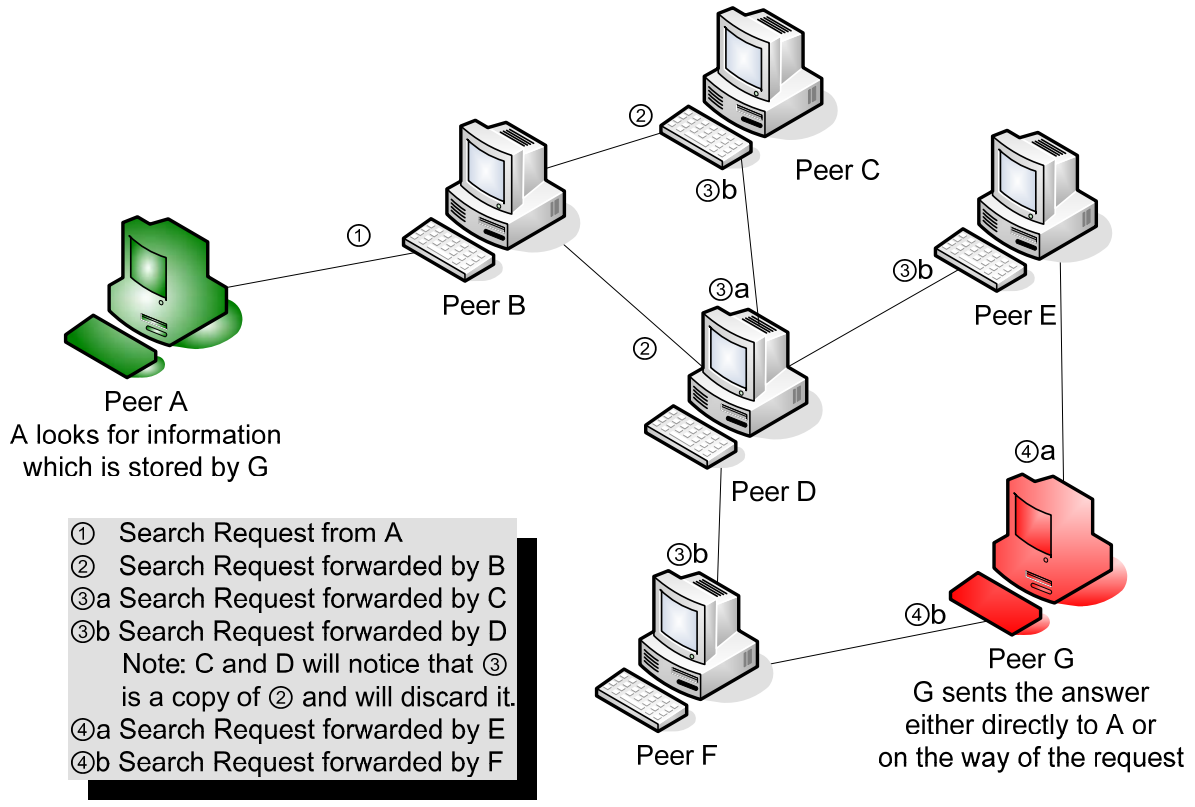

Figure 10: Pure P2P based system using the Flooded Request Model for information retrieval

Examples of the more dynamic hybrid P2P based systems are networks where nodes with outstanding capabilities (e.g. available bandwidth or computing power) are 'elected' to offer special functionality to the 'normal' peers. This special functionality could be being part of the search infrastructure within the network - functionality 'normal' peers do not offer. Another common special functionality is to connect nodes which can not communicate directly otherwise (for instance because of firewall restrictions). The well known VoIP

service provider Skype™ uses these hybrid technologies. They call their special nodes 'supernodes'.

Besides the already discussed CDM for information retrieval (which implies a hybrid P2P network), the Flooded Requests Model was developed for pure P2P networks (see Figure 10). The basic idea is that each search request for a given piece of information would either be answered by a given node or this node will forward the request to all its direct neighbours. These neighbouring nodes will do the same so that in the worst case the whole P2P network gets flooded by the search request. Although this search strategy will always find the requested information (if it is available somewhere in the network) without the need for centralised directory nodes - the disadvantage of limited scalability overrules it.

The more peers joining the network and the more search requests they do, the worse the performance becomes and the more resources are needed. Therefore the FRM is suited only for relative small P2P networks with a limited number of participants. But the simplicity of FDM and the absence of complex routing or synchronisation protocols etc. makes it still appropriated for this case.

The original version of Gnutella is a prominent example for a P2P network which uses the FRM. But it also shows the performance problems mentioned above.

To overcome these scalability and performance problems of CDM and FRM on one side, but preserve the robustness of pure P2P based systems on the other side an alternative approach was developed. This approach is called the Document Routing Model and is based on distributed hash tables. P2P systems which use the DRM are often dynamic hybrid systems.

The basic idea of DRM is that each peer has a random number (NodeID) assigned to it. Every content (or piece of data) which should be published gets also a number (ContentID) assigned to them (usually this value is computed by applying a hash function to the data). The peers whose NodeID are 'sufficiently similar' to the ContentID are responsible for storing the content (or more general for storing information about the location of the content). If now a peer receives a search request for a given ContentID it tries to 'route' this request to those peers he knows about whose NodeID are 'close' to the ContentID.

The average search performance of DRM is O(log N); N is the number of peers (with a worst case performance of O(N)) making this a mechanism which scales very well with a growing number of peers.

After some piece of data was located, it needs to be transferred to the requesting peer. In a simple case this is done by downloading the whole information from exactly one peer. This is called single source file transfer. The biggest disadvantage of this technique is that the download speed is limited by the upload bandwidth of the offering peer. This becomes especially a problem in P2P based systems where the overwhelming majority of peers are normal home users with their asymmetric[33] Internet connection lines (such as ADSL).

To overcome this limitation the multi source file transfer (MFT) was developed. In its simplest form a peer just downloads different parts of the requested content form different peers. More sophisticated algorithms try to optimise the way the initial distribution of content is organised to ensure that the content becomes quickly available to all interested peers without overloading the initial contributor.

[33] Typically the available upload bandwidth is much less than the download bandwidth.

Figure 11 gives an example for these techniques. In a first step peer A sends parts of a file to peer B and peer C. Note that these are different parts of the same file. In a next step peer B and C can exchange their parts. Moreover A could also send an additional part to one of them. If later peer D takes part in the network, it can download simultaneously three parts of the file from A, B and C.

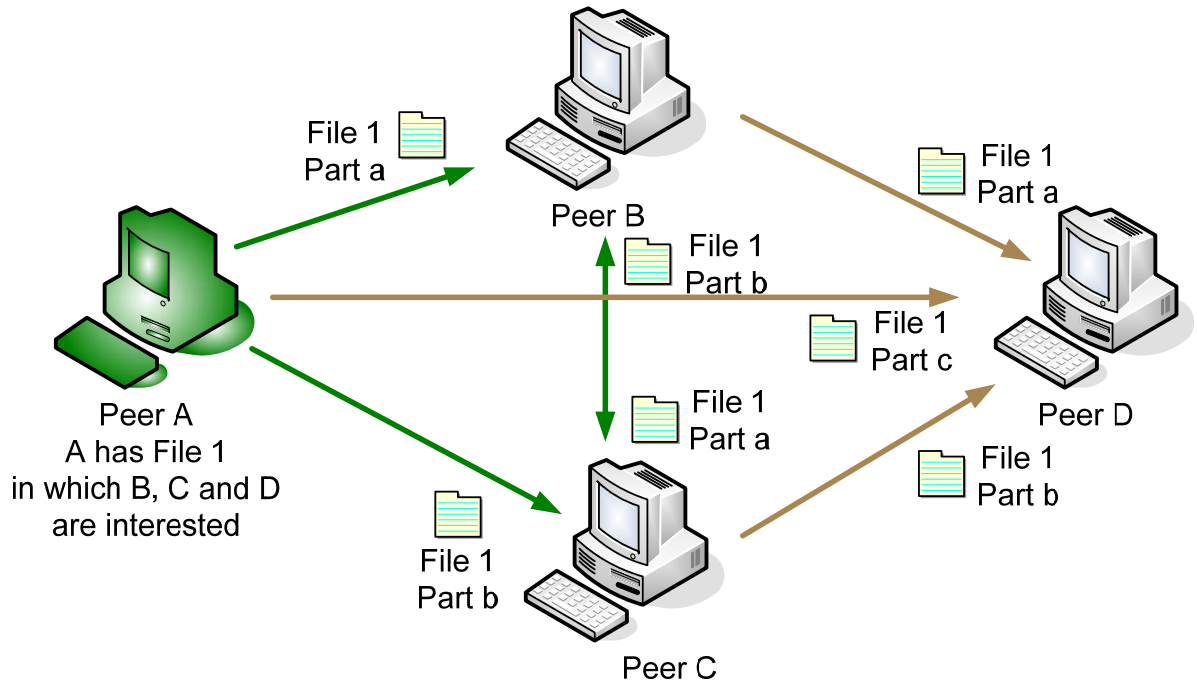

Figure 11: Multi source File Transfer within a P2P based system

A usual problem with P2P based systems which deals with content distribution is that often the peers are interested in downloading some data but not willing to provide upload resources. As a solution to this problem P2P networks can implement 'payment' (economic) or reputation systems. Various kinds of these systems exist. One of them is called 'Tit for Tat' strategy. It means that the amount of available download resources (e.g. in terms of bandwidth) depends on the upload resources a peer provides to others.

One of the relevant P2P networks and protocols which implements multi source file transfer and uses the 'Tit for Tat' strategy is called 'BitTorrent'. The BitTorrent network belongs to the category of hybrid P2P based systems. The basic idea is that all peers who are interested in a certain file form a logical group, which is called a *swarm*. A member of a given swarm is either a *seeder* or a normal peer. A seeder owns the file whereas normal peers only have parts of them. In order to coordinate the seeders and the normal peers a third component called *tracker* exist. A tracker manages information about which seeds are available for a given file and which peers have which parts. The tracker intelligently responds to requests done by the peers for parts of the file ensuring that all parts of the file are evenly distributed among the swarm. This intelligent management of swarm resources enables a BitTorrent network to distribute content very quickly and robustly.

The BitTorrent network itself does not offer any search capability. If a client is interested in certain content it needs a special file called *.torrent* which contains information about the tracker and some other meta-information necessary to start the download.

In contrast to many other P2P based system for content distribution (or file sharing) there does not exist one big BitTorrent network where all the content is distributed. Rather there will be created temporary swarms which then work together to share the content. The tracker is always in the position to pinpoint which content it will support and which not.

The last-mentioned property makes even 'serious' companies very interested in this technology. The computer game producer Blizzard uses BitTorrent to distribute beta version of their game 'World of Warcraft' among interested testers. Also all well known Linux distributions use BitTorrent for spreading their software. A new trend is the legally compliant distribution of media content (TV shows, movies etc.) using P2P based technologies, especially BitTorrent. The company Azureus Inc. achieved an agreement (content partnership) with the BBC Worldwide Limited (a subsidiary of the British Broadcasting Corporation (BBC). This agreement allows Azureus Inc. to offer BBC content (comedies, dramas etc.) to the users of its new BitTorrent based digital media platform called Zudeo.

The widespread usage of the BitTorrent protocol is supported by many different activities like integration of a BitTorrent client into the Opera Web-Browser, developing of special hardware chips enabling even limited (embedded) devices to utilise it etc.

Nevertheless BitTorrent and other P2P based content distribution systems are still stigmatised as illegal and for supporting of unlawful copyright violations. From a regulations and legal point of view it is absolutely necessary not to forbid or regiment a whole technology but rather use cases of certain applications of this technology.

As argued and explained so far, P2P based systems and especially networks are emerging technologies which are particularly useful for distributing content in a very cost-effective way. Therefore they are one candidate for the architecture of the communication backbone in upcoming AmI spaces.

Hence it is necessary to have a closer look at the identity and identification, privacy and data protection related risks linked to this technology. They are mainly the same as the ones mentioned in the Grid computing section: if the data is not appropriately secured (e.g. encrypted) then it could be revealed to all participating peers. Note that encryption or integrity protection is not a build-in feature of most of today's P2P based systems. Besides these confidentiality and integrity problems a peer (or a colluding group of them) could even try to profile a user. This is especially an issue with hybrid P2P systems, where some special (centralised) nodes are in a good position to do this.

More research is necessary to develop real privacy enhanced P2P based systems. But this requires that the society accepts P2P as a useful technology and will not hinder privacy researchers to enhance P2P systems.

3.3.6 Context aware software and systems

In the FIDIS deliverable D7.3 "Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence" it is stated that profiling is one of the central techniques necessary to build and provide sophisticated AmI space and the schematic view below is given (see Figure 12):

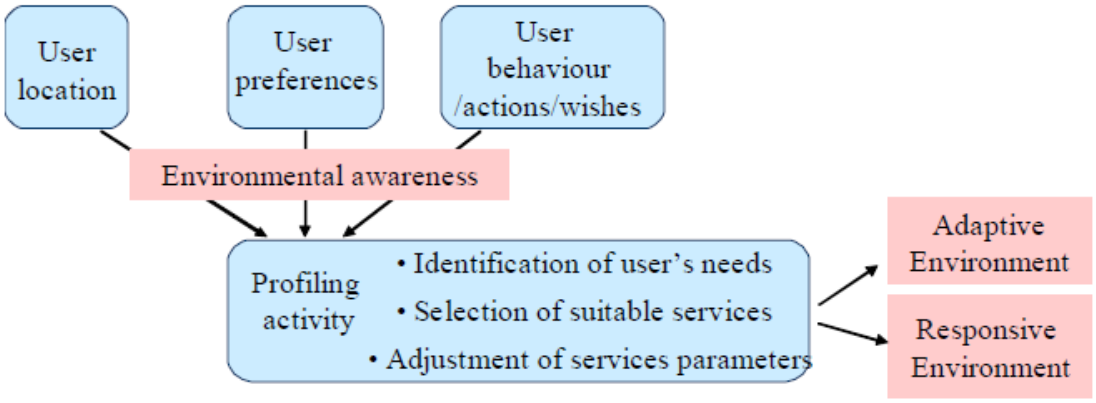

Figure 12: Schematic view of profiling activity in the AmI environment

Although an important part - profiling is still only part of the background processing that makes AmI acting 'intelligent'. A broader conceptual view on this is expressed by the techniques called *context-awareness* and *context-aware computing*.

First of all it needs to be clarified what the term *context* in the area of context-aware computing means. Actually a lot of different definitions exist which all cover different aspects of the concepts related to context in the field of computer science and computation. A general and intuitive definition is given in [Lieberman *et al*. (2000)] describing it as "… everything that affects the computation except the explicit input and output …".

As refinement of this very general definition, approaches could be found which try to specify categories of information that set up the context. Examples of these categories could be the user's location, social status or behaviour properties of the environment including capabilities of computing devices etc. (see also Figure 12). Some authors even try to build complex hierarchies of these classes of information [Schmidt *et al.* (1999)].

Nevertheless these 'enumerative' approaches have the disadvantage that they are very domain and application specific. To overcome this limitation a more conceptual definition of the term context was developed. The following definition taken from [Franz *et al*. (2007)] tries to unify these definitions and to establish a common notion for the term 'context':

***Context** is the state of an entity's environment related to its activities. The part of the potentially available information which is considered to be relevant for influencing or triggering these activities will be described by a model.*

The model defines

- *which features are potentially considered to describe the state,*
- *whether these features are directly or indirectly derived from measurements provided by physical or virtual sensors,*
- *dependencies between these features,*
- *dependencies of features from former states, and*
- *how to draw conclusions about the state based on these features.*

An instance of this model describes the current state of the entity's environment.

Given this definition, the authors of [Franz *et al*. (2007)] concluded that context-awareness could be defined as follows:

***Context-Awareness** means that activities of an entity are influenced or even triggered by knowledge of the current context. A characteristic feature of context-aware systems is the aim to support interactions between an entity and its environment.*

As it could be seen from these definitions profiling and the environmental awareness combined with the related reactions as shown in Figure 12 are just some aspects (or a refinement) of context and context-awareness.

The following example may illustrate this: The foundation is the scenario of the AmI bar as described in the FIDIS deliverable D2.2. On the one side the AmI bar has to perform all kinds of profiling techniques to find out that a certain guest of the bar usually orders a certain type of beer. But knowing this profile alone is not sufficient for an 'intelligent behaviour' of the AmI bar. It needs more *context information* - especially which types of beer are in stock - to react appropriated using context-aware computing. Thus the profile is part of the context.

The FIDIS deliverable D7.3 discusses extensively the implications and risks coming from profiling and describes known solutions at technical, sociological and legal level. As context-aware computing can be understood as enhanced version of the profiling related processing techniques at least the same problems regarding identity, privacy and protection of personal data can be foreseen.

Besides what is already described here, we want to concentrate on context-aware computing as emerging and enabling technology for privacy enhanced AmI space. As discussed in Section 3.2.8, in a privacy enhanced AmI space the fixed sensors of the environment should emit information about themselves. These huge amounts of unstructured data need to be filtered and pre-processed in order to inform (or even react on behalf of) the user in a non-annoying manner. Context-aware computing seems to be one key technology to achieve this goal. The personal device of the user (responsible for informing him) needs to be aware of the current situation, user's preferences etc. (hence the relevant context) to make 'intelligent' decisions very similar to the way the surrounding AmI space makes its decisions.

Because AmI environments are somewhat speculative things of the future, the usage of context-aware computing to support PETs is illustrated below on the most elaborated example of collaborative eLearning[34].

Regarding privacy, collaborative eLearning is very contradictory: on the one side users want to work (learn) together e.g. by aiding each other, which usually requires a lot of information about the different participants. On the other side a user might not want to disclose too much information about himself, in order to avoid being associated with under achievement etc. This becomes especially more complicated if the user is a member of different learning groups.

BluES'n is an example for such a collaborative eLearning environment, which is based on workspaces, in which users can learn and work together [Borcea-Pfitzmann *et al*. (2005)]. From a privacy point of view a partitioning regarding disclosure of information related to the different workspaces is necessary. This can be achieved by intra-application partitioning (IAP) as described in [Borcea *et al*. (2005)]. However IAP so far uses classical identity

[34] The statements are a summary of the example given in [Franz *et al*. (2007)].

management technologies, which require the user to *choose* a particular partial identity for every relevant situation. Drawbacks of usability are the shady side of this because:

- IAP must be applied additionally to the primary tasks the user wants to perform and
- The accruement of data and their influence on privacy are often not obvious to the user.

Therefore context-aware computing is used to support the user. Especially two aspects are of importance:

1. Raising of privacy awareness by informing the user continuously about his privacy state and
2. Supporting of the usage of IAP by making automatic decision (or at least suggest them) based on the current context (which covers the user's privacy preferences).

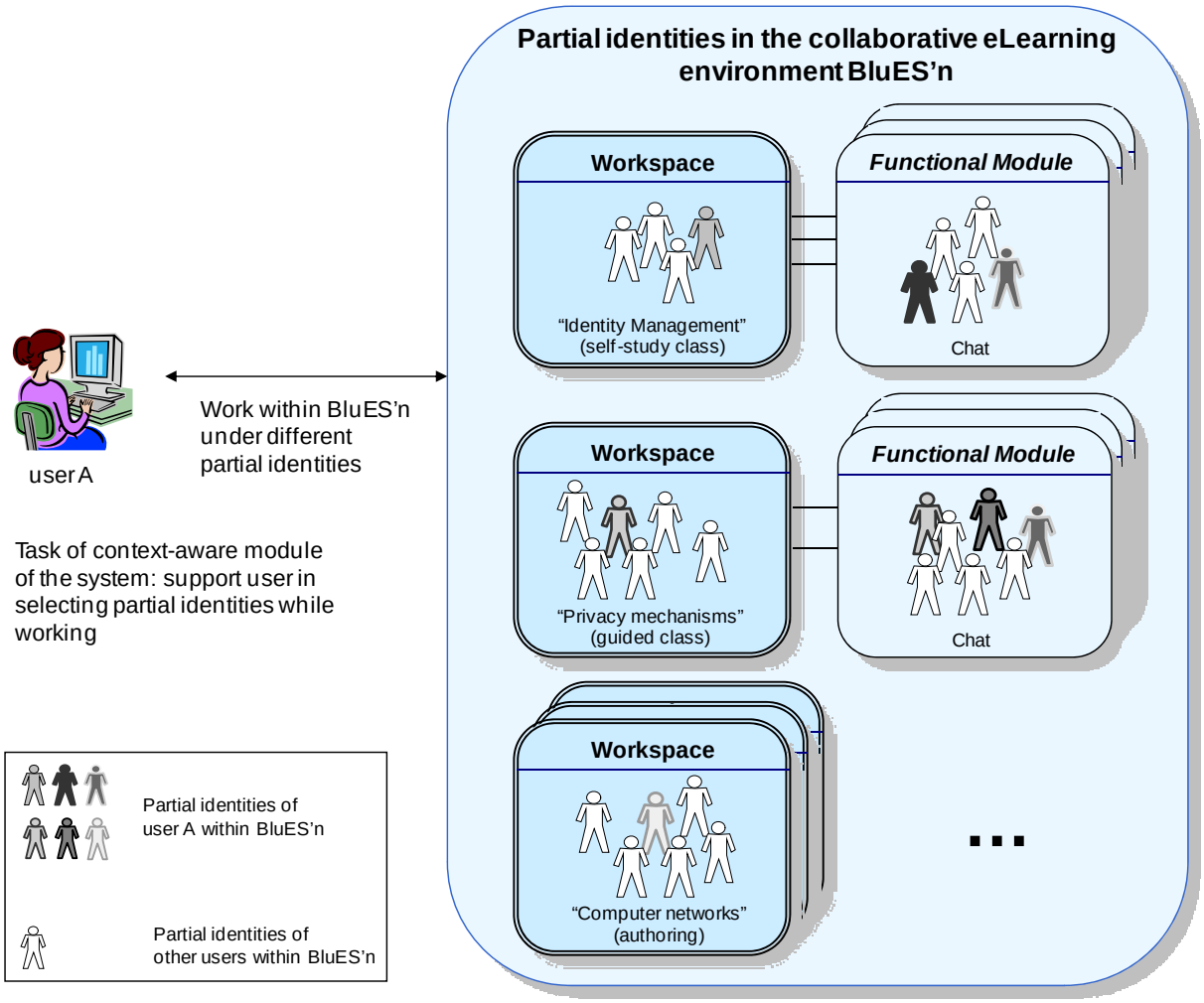

Figure 13: Context-aware computing to support privacy - illustrated by the collaborative eLearning environment BluES'n [Franz *et al.* (2007)]

Within BluES'n a context-aware component called Decision Suggesting Module (DSM) is responsible for these tasks (see Figure 13). Particularly, the DSM has to evaluate the current context and to generate a suggestion (or to make an automatic decision) regarding which partial identity an initiated action should use [Franz *et al*. (2006)]. All information related to this action - data requested by the server due to access control policies, data explicitly sent by the user, but also information about the action itself - can be assigned to this partial identity. Additionally, relevant contextual information will be presented in a privacy aware user interface [Franz *et al*. (2006a)].

However, one also has to consider that users want to be recognised by others in a collaborative scenario to enable reasonable working. Thus, it is not possible to perform all actions anonymously or under different partial identities, respectively, to ensure their unlinkability. The DSM has the challenging task to support these two oppositional goals. As already said it is of course necessary that the user defines his preferences regarding these goals since this cannot be done automatically.

3.3.7 New Shapes for Computational Devices

A number of trends in technological development will lead to new shapes for computational devices. In this context the most important ones seem to be:

- Miniaturisation of integrated circuits (ICs)
- Integration of more and more functions (e.g. increased computational power, communication using different types of networks, network protocols etc.)
- Development of new and smart materials

Early examples are, for example, new shapes of RFID tags integrated into clothing. Far more advanced are wearable computers that integrate computational systems, interfaces and displays in clothes [Lisetti and Nasoz (2004)].

Other examples for new shapes are mobile devices with more and more integrated functionality. Already today PDAs can be used as mobile phones, computers with office applications, web-surfing devices, and media players. Integration of additional functions will increase in future.

Since 1997 Pister *et al*. carried out research at Berkley University with the target to develop self-contained, millimetre-scale sensing and wireless communication devices (so called motes) for massively distributed sensor networks. A number of these wireless connected motes are called Smart Dust. The working group of Pister suggested many different areas of use for Smart Dust, many of them with a military or secret service background.[35] Recently, Steele (2005) summarised state-of-the-art in Smart Dust related research, development and application.

New shapes for computational devices will play a major role in the context of sensors, actuators and computational devices for AmI. They also may be used for advanced identity management devices, based on today's PDAs.

[35] See http://www-bsac.eecs.berkeley.edu/archive/users/warneke-brett/SmartDust/index.html

Research seems to be driven by public as well as private organisations, depending on the planned use of the resulting products. While mobile phones and PDAs currently are developed by private enterprises, in the area of Smart Dust research mainly seems to be driven by public research institutions.

3.4 Conclusion

The concept of AmI is largely based on the idea that by augmenting an environment with sensor technologies and by providing near unlimited storage and processing capabilities, the intentions, needs and desires of people can be predicted and catered for. The result is that people will not need to know how to operate complex technologies – instead the technology will interact with them in intelligent and intuitive ways. Clearly collating information is the key. However, if an environment is to know what a person wants or needs without being explicitly told, then this information needs to come from indirect means – i.e. the technology, or rather the environment as a whole becomes less interactive, and more proactive. Through varying levels of sensor data gleaned from pervasively embedded sensors, dynamic autonomic profiles can be drawn to enable this proactive ability. Intuitively these profiles can only be as good as the data that feeds them, and the processing available to create them, and hence the focus of development is to extract as much data as possible from all aspects of the users and their interactions within an AmI space, as well as developing the underlying infrastructure through which this data can be 'mined' for new information.

Here we have presented a range of technologies which are considered applicable in the fabric of an AmI environment. These stem from fundamental sensor technology for AmI spaces which will enable the data capture from which new information can be inferred, to enabling technology, i.e. technology which will serve in the underpinning infrastructure to provide the networking and processing capabilities necessary in the envisaged future scenarios of augmented living. Notably, and in contrast to other texts on AmI related technology, we have also presented the concept of 'sensors which detect sensors' which may prove to be a way in which our privacy can be conserved to a greater extent in environments where data capture becomes ubiquitous.

In any case, it is clear that the user and the controller of the data are not one of the same. Indeed in some cases it may be unclear who is collecting data from sensors and what it is being used for. One route to counteract such issues is the idea that new technologies should incorporate 'privacy by design', that is the mechanisms necessary for user control of their data should be an inherent aspect of the technology. To this end, many privacy advocates have suggested that emerging technologies and applications should undergo mandatory privacy assessments before they are released into the mass market. To a large extent the technologies discussed above are speculative in that, in the main, they have not reached a mature level of development or deployment. Thus, it is exactly at this point where such technology needs to be discussed beyond the domain of those creating it to ensure that we are able to stay in control. 'Staying in control' is a broad turn of phrase, and indeed its exact meaning and context here is open to interpretation. However, what is for sure is that there are fundamental rights and freedoms which must be ensured with the development of any technology and, with this in mind, in the next chapter the technologies discussed above will be considered from a legal and ethical standpoint.

4 Fundamental rights and emerging technologies

"*We, the representatives of the peoples of the world, assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilise and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.*" [36]

4.1 Introduction

In this chapter, we will assess some of the new and emerging technologies described in chapter 3 from a legal and ethical viewpoint. The starting point for this short prospective analysis will be twofold: we will only assess some of the emerging technologies on the basis of the European *Charter* of Fundamental Rights and Freedoms[37] and we will assess or rather *challenge* such technologies with an exercise of *questions and remarks* instead of with answers. Our approach can thus be called an approach of 'infoethics'.[38]

There are many good reasons to use the *Charter* to assess emerging technology. First, we think that fundamental rights and freedoms in general have been approached too little in analyses with regard to future and emerging technologies so far, although all fundamental rights and freedoms - and not alone a right to privacy - are paramount for our Western even intercontinental concept of identity; the scope of the articles in the *Charter* will show that the possible problems and issues regarding human rights and freedoms go so much further than the actual - sometimes artificial - privacy perspectives alone. This FIDIS deliverable offers us the great opportunity to take up other rights and freedoms included in the *Charter* that will play an important role with the introduction of new technologies in society, such as the right to human dignity, to the integrity of the person, the presumption of innocence, the prohibition of slavery, the freedom of assembly, of speech etc. Second, the *Charter* differs somehow from other international legal texts since it clearly puts a *European* stamp on rights and freedoms by including chapters on 'solidarity' and 'equality' that have more intercultural and social aspects (so-called third generation rights, in articles on cultural diversity, integration of persons with disabilities, right to access to services of general economic interest, social assistance, health care, environmental protection...). Thirdly, however, the *Charter* does not lead us away at all from important questions regarding privacy, data protection, intellectual property and consumer protection, because all these rights are maybe abstractly but nevertheless explicitly included in it. Fourthly, the *Charter* being written in more abstract language and consisting of articles that are rather promising than concretely and immediately

[36] Article 1 of the "Geneva Declaration of Principles" of 12 December 2003 (Declaration of Principles. Building the Information Society: A Global Challenge in the New Millennium), United Nations *World Summit on the Information Society* held in Geneva 2003 and Tunis 2005, see http://www.wsis.org.

[37] Charter of Fundamental Rights of the European Union, 7 December 2000, *Official Journal* C 364, 18 December 2000, 1-22. This Charter has not become into force (yet) since it was part of the European Constitution, which is still not entered into force because, amongst other reasons, the people of some Member States of the EU rejecting the Constitution in a referendum.

[38] On the term *infoethics*, see below.

applicable and enforceable, such a general formulation of rights and freedoms allows to approach emerging technology also from a more abstract and conceptual view: at the stage of development, this more abstract approach may be a better approach than rather anticipating concrete and often specific case-related cases that do not have a general impact on the EU policies.

Why asking questions while not trying to give a concrete answer? Of course, the main reason is that it is too early (and maybe too presumptuous) to give legal answers for emerging technologies that are (as we at least assume) not or not completely deployed in the information society market yet. By then, technology may change and adapt to fit so that the answers of today are not valid any more tomorrow. Will interconnected RFID readers ever be placed in streets and shopping centres to read out the identity of people? If yes, what will be read and where will such information be stored, and who will have access to such information in which circumstances? Will we ever be able to detect emotions or criminal thoughts through BCIs? Will there exist *one* database with the biometric templates of all people to which all private access controls in a city are linked? To what extent will our life and online identity development depend on Grid computing? However, the ethical and legal questions will be implicitly based on certain pictures or scenarios we make in our dreams of the future information society. Scenarios are only imaginative stories about what the future might be like and help us to plan: they are not predictions, but tools for preparation [Garreau (2004)]. They can "anchor the design process, at the same time as evoking reflection, and focus that reflection on situations of use, both as they occur in the real world and in the future" [Welen *et al*. (2004)]. Finally, questions may sometimes survive much longer and have a more profound impact on the awareness of scientists and policy makers. At the end, discovering questions that seem to always return when looking at new technologies may provide us with a broader picture that can be much more useful. And that is what we try to achieve in this chapter.

We will base thus our analysis on some of the emerging technologies already described in this deliverable. The *Charter of Fundamental Rights and Freedoms* consists of five chapters which are entitled Dignity, Freedoms, Equality, Solidarity, Citizens' Rights and Justice. It contains a total of 54 articles and it can be consulted directly online.[39] We will indicate for a technology one or more specific articles for which questions may arise. This overview is far from exhaustive; it is rather meant as a starting point for contemplation.

4.2 Context: Infoethics

What is attempted in this chapter is to raise normative questions in relation to emerging technologies, in particular ones that are triggered by fundamental rights. This is one step in a much wider analysis that should be undertaken, namely to investigate the normative – ethical and legal – questions raised by emerging technologies. This wider context can be designated as *Infoethics*, a term also used in a recent UNESCO paper that deals with similar questions as this chapter. The fact that UNESCO is investigating infoethics only serves to prove the increasing importance of technology-related questions with regard to human rights and freedoms [Radoykov *et al*. (2007)].

[39] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

As the UNESCO paper explains, infoethics is the application of ethical principles with regard to the development and use of information and communication technologies. Such technologies seem to keep on emerging and form one of the basic structures of the European information society. They have thus a tremendous impact.

Infoethics is broader than 'law'. Because of the super-fast development in ICT and the unstoppable experimentation in society itself, the traditional mechanisms of law – that work via policy makers or *legal politicians* who command legal text writers or *legal technicians* to write law according to their politics – can only intervene at the moment a particular technology with all its short-term advantages at micro-level has been put in the market.[40] Since the law can often intervene only after technology has been put in the market, the intervention with regard to the possible negative impact on a long term macro-level, should in order to be effective not be purely legal at a post-production level, but should also take place in an earlier stage during the production of the ICT and at different levels. This can be achieved by actions that go beyond law alone. Examples of infoethics instruments to be used by policy makers, lawyers, scientists, developers, economists, CEOs, sociologists and even the consumers themselves, are self-regulation, industry standards, ethical codes, codes of conduct, user awareness programs and so on. In this chapter, we investigate one part of this broad field: the role of fundamental rights for emerging technologies.

4.3 Fundamental rights and emerging technologies

4.3.1 Simple Sensors

As described, sensors and particularly remote sensors can have an important impact on privacy and data protection where the persons concerned are not at all aware that information relating to them is remotely perceived. In addition, the mere presence of sensors in public places, even if noticed, does not inform about important facts such as who is controlling the sensors, which information about them is 'sensed', for which purposes the data are used by whom and in particular: are the data stored or are they immediately 'forgotten' when not needed for the particular purpose? (article 7 and 8).

UNESCO indicates that information derived from such sensors is very useful but often appropriated although such information belongs to the public domain. Where information is obtained from sensors put in the public domain, such as market places or even earth images captured by a satellite, such information should be readily available to anybody. There are many ambiguities on how the vast amount of benefits of public domain sensor information will be shared (article 11 - freedom of information) [Gutwirth (1993)].[41]

How will the freedom of speech and particularly the freedom of expression respond to sensors that are programmed to detect abnormal, deviant behaviour and then to react correspondingly (starting to record, triggering an alarm etc), e.g. when someone has a strange voice, walks into the opposite direction, screams to the other street side to say hello to a friend, staggers etc.?

[40] With micro-level is meant the technology itself as a stand-alone production, viewed outside and not dependently on the complete picture of the role of the collection of all technologies in our society.

[41] GUTWIRTH analyses how information, revealed by remote (satellite) sensing of raw materials like oil and ore, is only available to rich industries, which puts developing countries as a consequence of unequal access to information about the public domain in an unfair position at the negotiating table.

How does the freedom of expression in a sensor-world - that is almost committed to objectify the environment as much as possible - relate for example to the freedom of speech, including body language (article 11 - freedom of expression)?

Article 21 of the Charter explicitly prohibits "any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, (…), property, birth, disability, age or sexual orientation". How will a technical possibility - and in fact the exact functional design of sensors - to 'sense' sex, race, colour, genetic features, language, disability, age or other features and to subsequently respond differently on the basis of such characteristics, influence the fundamental principle of non-discrimination? How then must discrimination be understood in a society where computers will make automated decisions on the basis of such characteristics?

4.3.2 Radio Frequency Identification

RFID is already being extensively discussed in law, science & technology, and society, particularly with regard to privacy (article 7). But the impact goes much further. What impact does a massive deployment of consumer products with mere small and passive RFID tags have with regard to fundamental rights and freedoms, when such tags only allow for unique identification and location of such products? We assume problems with regard to data protection in the first place: what information is on the tag, when is the tag being read and by whom and for which purposes, to which information is the information on the tag linked? Is it by the way necessary that the information on an RFID tag falls under data protection law in order to enjoy the right to be informed, which information can be read from the product you possess (article 8)?

There will be many questions with regard to consumer protection (article 38), such as whether companies can impose that RFID tags must remain attached to the products in order to receive product guarantee, hereby circumventing a possible right of the consumer to remove the tag once the product is bought.

What about environmental protection, if billions of products - of which so many are meant to be thrown away after consumption - are equipped with small silicon? (article 37)

Are the right to security of people, as granted by article 6 of the *Charter*, the right to healthy work environment (article 31 para. 1) and the "high level of human health protection" (article 35) safeguarded, when it is not a hundred percent sure, whether radio waves - in mega-quantities as will surround us in an RFID-enabled AmI world - are healthy or dangerous for us?

4.3.3 Brain-computer interfaces (neural signal processing)

Article 8 of the Charter provides for a fundamental right of protection of personal data and hereby states that personal data may only be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law". Brain-computer interfacing (BCI) allows processing of neural signals and it is assumed that neural signals may indicate - even represent - thoughts. The Guardian reported in 2007 that "a team of world-

leading neuroscientists has developed a powerful technique that allows them to look deep inside a person's brain and read their intentions before they act".[42]

Under what conditions can the neuro signals be considered creative and specific enough to invoke intellectual-property rights (Article 17 para. 2)? Can certain thoughts, when registered by a brain-computer interface, be a work of invention that falls under copyright law? Or can a sequence of neuro-signals, for example, a sequence that invokes a happy, yellow feeling in the brain, be patented by the 'thinker' of these signals?

In our assumption that brain-computer interfacing evolves in such a way that neural signals can be detected and that these 'data' give various kinds of 'information', a wide range of questions concerning the acceptability of brain 'reading' arises. One question is whether processing of neural signals (personal data) without consent of the data subject (thus on the basis of another legitimate basis) can be lawful in any situation. If yes, what situation would that be and under which conditions? For example, can employers (such as schools afraid of hiring paedophiles, or intelligence services screening personnel for infiltrators), insurance providers, or the police (lie detection) ever be allowed to compulsorily process brain signals?[43] Can any individual - convicted or not - ever be obliged to have his cortex connected to a machine without consent?[44] These questions are not only relevant in light of Article 8 (data protection), but also – and more so – in light of Articles 7 (personal life), 3 para. 1 (physical and mental integrity), 1 (human dignity), and 10 (the freedom of thought, conscience and religion).

The freedom of thought, conscience and religion, human dignity, and mental integrity are not only at stake through brain 'reading' but also, even more poignantly, through the reverse process, brain 'writing', i.e., inputting neuro-signals to the brain to trigger certain behaviour, thoughts or feelings. Should law enforcement be allowed to send a 'stop leg motion' signal to the brain of a convict who tries to escape while on probationary leave? This would be an extreme infringement of the human rights mentioned. More complex is the question whether someone could voluntarily agree to have his brain altered through neuro-signal processing.[45] This is readily accepted for patients with Parkinson's disease, since neuro-stimulation can suppress a substantial amount of its symptoms. But how do we feel about persons having their brains altered in the way of *A Clockwork Orange*, to eradicate paedophilic or aggressive

---

[42] THE GUARDIAN, "The brain scan that can read people's intentions", 9 February 2007, http://www.guardian.co.uk/frontpage/story/0,,2009229,00.html. See also Stephan Schleim, 'Lauschangriff auf das Gehirn', 10 May 2007, http://www.heise.de/tp/r4/artikel/25/25256/1.html.

[43] *See* US patent 2002188217 (inventor Lawrence Farwell) entitled "method and apparatus for brain fingerprinting, measurement, assessment and analysis of brain function" on the use of neural signal processing for the specific purpose of criminal investigation (*see a.o. the third claim of the patent)*. The technology has been successfully used to discover the FBI agents within a group of people. The abstract states: "Electrical signals originating in the brain are measured and analyzed. In one embodiment, this technology serves to assess brain functioning as a means to evaluate cognitive functioning, to detect cognitive deficits such as those brought about by Alzheimer's, and to assess the efficacy of treatments for cognitive disorders. In another embodiment, which is an improvement on technology previously patented by the inventor, this technology serves to detect information in the brain as a means of detecting participation in specific organisations, acts, or criminal activity. In a third embodiment, this technology serves to evaluate the effectiveness of advertising, educational and training presentations by detecting the attention, information processing, and memory-related responses to these presentations as revealed by brain waves". See http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=US2002188217&F=0

[44] NEW SCIENTIST, "Neural 'extension cord' developed for brain implants", 19 January 2007, http://www.newscientisttech.com/article/dn10997-neural-extension-cord-developed-for-brain-implants.html.

[45] Scientists reported in March 2007 that they succeeded in erasing traumatic memories from rat's brains. However this was not done by ICT but by a chemical substance, see [Doyere *et al*. (2007)].

inclinations? The question rises to what extent this can be really voluntary (e.g., if someone faces a choice of five years' imprisonment or brain treatment) and whether consent is ever given in an informed way (it being very hard to oversee the consequences). Also, given that this type of brain stimulation may be prone to change the identity of the person (there are indications for this with current treatments of Parkinson patients), should society allow this to happen at all, given the primacy of human dignity (Art. 1) and the fact that the sense of self (*ipse identity*) resides in the brain?

If neural signal processing generates data that can be considered as certain thoughts, can someone ever infringe a criminal law purely on the basis of thoughts? Can someone ever be convicted merely by 'thinking' something, if such thinking can be traced by neural signal processing? Currently, criminal law only penalises activities, even if more and more acts are penalised that are not criminal in themselves but which prepare the way for crimes. Conspiracy, preparatory activities, misuse of devices (Art. 6 Cybercrime Convention), and jihad recruitment are examples of this. A next step could be, if neurotechnology allows the discovery of intentions within the brain, to penalise intending to commit a crime. Also, like current law penalises certain types of offensive material (child pornography, racist statements, and in certain countries holocaust denial), one might consider whether criminal law should be extended in future to also include 'criminal thoughts'. Should thinking of a child rape or thinking that the holocaust has never happened be punishable? And if so, should the remedy be to 'implant' in the brain the conviction that the holocaust actually did happen? In short, should criminal law be extended with punishable thoughts, with all its implications for human dignity, freedom of thought, and mental integrity? This, we think, is one of the most important questions for the 22nd century.

4.3.4 ICT Implants

Not all ICT implants will *a priori* endanger human rights, but ethical issues do surface when ICT implants can be read out remotely, or when such implants are used for goals that escape consent or control by the person concerned.

Article 8 provides for a fundamental right of protection of personal data and hereby states that personal data may only be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law". Body-Computer Interfacing and particularly implants allow processing of body traits and it is assumed that body signals may indicate - even predict - emotions and behaviour. The Observer reported in 2002 that British Government considered implanting tags in convicted paedophiles that would be able to monitor the heart rate and blood pressure, hereby "alerting staff to the possibility that another attack was imminent".[46] In our assumption that body-computer interfacing through implants evolves in such a way that concrete information can be detected upon body signals, our question is whether any Court that will deal with the interpretation of this article may conclude that processing of body signals (personal data) without consent of the data subject (thus on the basis of another legitimate basis) can be lawful in any situation? If yes, in what situation would that be and under which circumstances (article 8)?

[46] THE OBSERVER, "Surgical tags plan for sex offenders - Silicon chip to be inserted under skin", 17 November 2002, http://www.observer.co.uk/politics/story/0,6903,841827,00.html.

This particularly relates to the presumption of innocence and the right of defence in a fair trial: what is presumption of innocence if technology intervenes a priori, *before* an unlawful act is committed? What if I am preventively but automatically arrested when an intelligent camera detects my aggressive behaviour? The question arising from Philip K. Dick's story filmed in 'Minority Report' - where a police department called 'pre-crime' apprehends (presumed would-be) criminals based on foreknowledge provided to the police department by 'pre-cogs' before the crime is even committed – seems suddenly not irrelevant at all (article 47 and 48).

To what extent can having an ICT chip implanted be an obligation *de facto* or *de jure*? What if participation to the information society necessarily supposes the implantation of an ICT device to have access to the necessities of life including food and shelter? [Radoykov *et al*. (2007)] What if just entering a city or enjoying emergency health care depends on having a chip implanted with respectively an identity number or a DNA fingerprint on it?

If the implantation of a tag is legally or even contractually imposed to have access to a product or service (particularly when there is a *de facto* monopoly such as being an emergency service), is this not an infringement of the right to human dignity (article 1 - people may find it horrible to have some silicon in their body), the right to physical and mental integrity (article 3 - respectively with regard to bodily and brain implants), the prohibition of *degrading* treatment (article 4 - leading to a distinction of humans and cyborgs, if cyborgs are considered to be of a higher grade because they enjoy more rights factually and even legally), the right to *liberty* (article 6 - is someone free when he must wear an un-removable chip), the right to privacy (article 7), the right to protection of personal data (article 8), the freedom of thought, conscience and religion (article 10 - brain implants may impede the freedom of thought, unlawful thoughts may be detected), the freedom of expression (article 11 - the ICT implant determines the expression which is not controllable by the subject), the rights of the child (article 24 - depending on the age when the chip is implanted and whether the parents can decide over the child) and the rights of the elderly (article 25 – depending on whether children can decide over parents)?

Many questions with regard to implants have something in common. ICT implants make it possible to store and process information inside, outside, towards and coming from the human body (and brain). The question is whether there will remain a difference whether data will be present (stored or processed) inside or outside the body. If law enforcement agencies today have already access to data processed by electronic communications not only between people (phone calls) but also between people and objects (websites, browsing information), will they have the right to have access to the same data when they are stored inside the human body? If law enforcement agencies have access to the hard disk of someone who browsed child-related pornographic places on the Internet, will such law enforcement agencies also have access to the hard disk, when the hard disk is implanted in the person? Should an ICT implant be considered to fall under the right to property (article 17 para. 1) or under the right to physical integrity (article 3 para. 1)? If the merger between body and ICT takes place in the sense that the internal body and/or the internal brain are connected to external computers and processors, does the difference between 'public' and private' - that is crucial for privacy - still make sense?

The European Group on Ethics in Science and New Technologies (EGE) has already produced an Opinion to the European Commission [EGE (2005)] entitled "Ethical Aspects of

ICT Implants in the Human Body" in which such questions as above have been dealt with (also with a special emphasis on the precautionary principle).[47]

4.3.5 Peer-to-Peer network architectures

Article 12 foresees the freedom of assembly and of association. Can the use of peer-to-peer technology be considered as 'assembly' and can the interdiction to use a peer-2-peer network or system be ever considered as an infringement to exercise the right to freedom of assembly?[48] How will this right to assemble and associate be valid for virtual assemblies and virtual associations? Does the data retention directive not infringe this freedom?

The same applies with regard to Articles 10 and 11 (freedom of thought, conscience, religion, expression and information). How can the freedom of thought, expression and information still persist when such activities take place in cyberspace, a place where each activity seems to be monitored and an increasing amount of data be stored? Will there be places like churches or bathrooms on the Internet, where someone can enjoy the same freedom as he has within the walls of his room?

4.3.6 Second Life and virtual worlds

Many questions can be asked in relation to the emergence of virtual worlds, such as Second Life. For example: are avatar data personal data of the person behind the avatar (art. 8), does the right to physical and mental integrity extend to avatar integrity (article 3), who has intellectual-property rights over the avatar and virtual things created by the avatar (article 17 para. 2), how is the freedom of assembly and association given shape in Second Life (article 12), is expropriation of an avatar an inhuman or degrading treatment of the person behind the avatar (article 4, 19), and is expropriation of an object (such as an expensive island or dragon sword) in Second Life a violation of the right to property (article 17 para. 1)? What will be the impact on people's behaviour and sense of identity of facts like news reports of the Belgian police starting official investigations (including police patrols) in Second Life as a result of a virtual rape of a female avatar?[49]

4.4 Conclusion

UNESCO defends infoethics as the fundamental priority of putting technology in the service of human rights.[50] Humans should take advantage of technology, not technology of humans.

---

[47] The Report refers to additional legal human rights instruments such as the Council of Europe Convention on Human Rights and Biomedicine, signed on 4 April 1997 in Oviedo, and the Universal Declaration on the human genome and the rights of man adopted by the UNESCO on 11 November 1997.

[48] On 22 July 2005, the Frankfurt local court (Germany) stated that an online demonstration (electronic 'sit-in') is not protected by the freedom of assembly; see Thomas Hoeren and Anselm Rodenhausen, 'Constitutional Rights and New Technologies in Germany', in: B.J. Koops *et al*. (Eds.), *Constitutional Rights and New Technologies*, The Hague: Asser Press (forthcoming).

[49] "Federal Computer Crime Unit patrouilleert in Second Life" [Federal Computer Crime Unit patrols in Second Life], *De Morgen* , 20 April 2007, http://www.demorgen.be/dm/nl/nieuws/multimedia/439275.

[50] Radoykov, B., Rundle, M., Conley, C., *Ethical Implications of Emerging Technologies: A Survey*, Paris, Unesco, 2007, 92 p. 11, http://unesdoc.unesco.org/images/0014/001499/149992E.pdf.

Respect for fundamental rights and freedoms is essential. It is not only privacy and data protection that are at stake and the discussion on security forms only a (temporary) part of the wider debate on how to live in tomorrow's information society. The promotion of a public domain for people having access to a diversity of information is essential within the development of emerging technologies. Respect for human dignity and equality and the freedom of thought, conscience and religion as well as the freedom to express, move, associate and assemble are only some of the rights and freedoms that are essentially at stake, where such activities suppose the increasing intervention of ICT and converging technologies provided and controlled by third parties.

5 Emerging Technologies and Society

Clearly we have adopted a technologically mediated way of living which inherently has far reaching consequences. Here we offer a forum for an initial inter-disciplinary discussion based on the complex issue of this technology evolution in its wider socio-cultural context. Following an initial statement on the topic from an anthropological perspective, we invited the responses of individuals and groups from the technical and legal disciplines. In this way we hope to contribute to the growing debate on the wider implications of emerging technology for our (continued) way of life. These statements can be considered personal and subjective rather than factual in the strictest sense. As such a short biography of each author is given to help set each discussion into its broader context.

5.1 An anthropological approach of technology and society: an overview

Daniela Cerqui

*Author's background***:** *Daniela Cerqui is a social and cultural anthropologist working at the University of Lausanne, Switzerland, and University of Reading, UK, involved in the study of the relationship between technology and society and, more fundamentally, humankind. Her research focuses on the development of new information technologies and the* '*information society*' *these technologies are supposed to create.*

Social and cultural anthropologists are involved in the study of differences between human cultures, and in the study of what human beings may have in common despite these differences. One common thing is the use of technology, as there is absolutely no human culture without it. Therefore, the study of the relationship between technology on the one hand, and society – and more fundamentally humankind – on the other hand, is a relevant topic.

Most anthropologists are more interested in other cultures than in their own. Nevertheless, our western society deserves being studied at different levels. As far as I am concerned, I am interested in the way technology is designed, produced, and used in my own society.

The main anthropological questions are related to what kind of society we want to live in, in the future. That implies a need to stand back from the classical visions of technology, which are, basically:

- Technological neutralism. According to this view, technology is neutral, and only its use can be good or bad. If you take a hammer to nail, it is good. If you take it to kill someone, it is bad. The user is the only responsible person for the good or bad result. The only thing we can do is to promote good uses.
- Technological determinism. According to this view, technology is intrinsically either good or bad. In the first case (technophile determinism), there is a faith that technology is the right solution for solving all the problems of the world (knowledge, wealth, and even happiness for everyone). In the second case (technophobe determinism), there is the belief that technology will lead us to a huge catastrophe.

Moreover, we very often find a mix of neutralism and determinism in common speeches. A good example is the World Summit on the information society. Organised by a Committee established under the patronage of Kofi Annan, the summit was initially mentioned in a resolution of the International Telecommunication Union, in order to be organised by the United Nations. It was held in 2003 in Geneva and in 2005 in Tunis. Most positions defended during the meetings assumed that we have no choice (determinism) and at the same time that we have to do the right things, if we want to reach the right goal (neutralism).

All these views have in common one thing: they consider that what has to be analysed is the impact of technology. It is taken for granted that technology does exist, and we 'just' have to assess its consequences. In other words, we have to wonder how to live with technology in the best way, considering that there are no other options. For instance, the discussions about privacy fall into this category.

Once a specific technology exists, we must indeed ask these questions, but the resulting debates are never-ending, unless we consider first the cultural context in which it was developed. An anthropological approach takes into account the society and its values as a whole. According to this holistic view, technology is never neutral. And neither is it deterministic.

It does not emerge from nowhere. Our values are embedded in it. Talking about impact and consequences is only one half of the problem, because technology is itself the result of a process. It is thought, built, and used according to principles that are taken for granted. Once it exists, it will reinforce these principles. Therefore, being responsible does not just mean being able to cope with consequences. Those who produce new technologies are at least as responsible as the users. The main question is related to what we develop these technologies for. What is the ultimate goal? Why do we want them? What implicit project for society and humankind are they part of? And only once we are aware of these long term issues, can we properly tackle the problems linked to how to live with technology.

To answer the question "why do we develop these technologies?", we need to know that all of us have a taken for granted definition of humankind, at two levels. First, we have a definition of what a human being is. That is so obvious for us, that most of the time it is difficult to detail it. Even more difficult: we also have a normative definition, i.e. an idea of what a human being should be.

All the technological devices are produced according to these two definitions, which are culturally and socially grounded. In other words, it means that they are the result of cultural choices. There are different ways of living together, and each society collectively defines its own rules. Generally speaking, society includes our social, our political and our economical systems. All of them continuously interact with each other, according to the main cultural values. Whatever the driving system is, it is shaped by these shared values. In such a context, the individual choices are subordinated to - and can hardly step out from - the cultural frame.

If we look further at our current values, we understand that our western society has clearly chosen a technologically mediated way of living. As we are convinced that there is no other option, we are diffusing it all over the world, where other cultures currently try to follow the same pattern, even if it is not their cultural one. According to people with power over our political or economical lives, as well as those from the scientific world, we are supposed to have recently entered the information era, which is supposed to be synonymous with an improvement in all the fields. French discourse talks of the 'information society' or the

'knowledge society', while English-speakers frequently refer to 'information highways'. All these phrases express differently the same idea: we are supposed to live in a radically new kind of society[51]. That so-called information Society is often considered as an unquestionable reality linked with the emergence and development of the Information and Communication Technologies[52]. With such a point of view, globalisation - defined as an extension of the Western information society to the entire world - has to become a reality in order to obtain a better quality of life for everybody. Information is described as the most important source of wealth for individuals and for countries (see for example [Gates, (1996)] and [Dertouzos, (1997)]) and it is expected to bring money and education to the whole world. That means that if, in the past, the industrial society needed efficient bodies to produce more and more, the information society needs nowadays efficient brains to deal with information. The keyword is: access. To be successful in such a society, you need to access information. And the quicker access, the better. Computers are nowadays put everywhere in our environment. They are becoming ubiquitous. But, paradoxically, they are also becoming less and less visible, by becoming smaller and smaller. Information technologies are also getting closer to the human body with each new breakthrough. Thereof, technological implants, brain to machine and brain to brain direct interfaces appear as the last logical step. If the device is implanted, there is no delay in accessing information.

According to Virilio (1995), the history of humankind has seen three major revolutions that point towards an ever-increasing speed in getting in touch with the world. The first one – in transportation – allowed humankind to master space by achieving the ability to move through it. The second revolution – that of transmission or communication – permitted a mastery over time, and allowed the elements of mankind's environment to reach him faster than if he was forced to move himself in order to obtain them. And the third revolution – that of transplantation – shortens the process even more by directly incorporating the information

[51] That is usually taken for granted, as the forthcoming shows. According to the World Summit on the Information Society web-site, which explains the challenge, "the modern world is undergoing a fundamental transformation as the industrial society that marked the 20th century rapidly gives way to the information society of the 21st century. This dynamic process promises a fundamental change in all aspects of our lives, including knowledge dissemination, social interaction, economic and business practices, political engagement, media, education, health, leisure, and entertainment. We are indeed in the midst of a revolution, perhaps the greatest that humanity has ever experienced. To benefit the world community, the successful and continued growth of this dynamic requires global discussion and harmonization in appropriate areas". The goal of the first step of the summit (Geneva, December 2003) is to try to obtain a consensual point of view (it is not easy to group the interests of different states, the business world and the civil society), and to develop some operative action plans. The second step (Tunis, 2005), focused on the evaluation of the results. http://www.itu.int/wsis/about/about_WhatIsWsis.html

[52] Contrary to what might be believed, such ideas are not so new. Some authors, see for example [Richta, (1969)], described the same concept without naming it or using another name many years ago. Bell was one of the first ones to theorise about that society while giving it a name: according to him, we are supposed to be in a post-industrial society [Bell, (1973, 1999)]. In his view, there are five fundamental criteria to define that society: (1) transition from a material goods production system to a service economy (mostly health, teaching, research and administration); (2) employment structures change with an increase in highly qualified professionals and technicians; (3) centrality of theoretical knowledge capable of generating innovation and economic growth ; (4) emergence of new technologies of the mind ; (5) an increasing mastery of technological and social developments.

In short, Bell describes an extension of the service sector, whose main condition of existence consists in the fact that information must constantly circulate. That explains the importance given to the information technologies.

into the organism.

With his experiments, Kevin Warwick [Warwick, (2003)] is just one step further than the rest of us. With the Internet, we merge metaphorically with technology. By interfacing his nervous system with a computer and the internet, he did it for real.

Coming back now to how to live with technology, we can think again about the problem of privacy, as it is valued in our society. IT must by definition be transparent. But this value is contradictory with the respect of the private sphere. Until we are aware of that, we will never solve the problem, because each coin has two sides. In this case, either the information must circulate without any boundaries and everybody can access everything in real time, or we want our privacy to be preserved. But we cannot have both.

5.2 Reply 1: "*Converging technologies, society & privacy*"

Eleni Kosta, Diana Bowman & Bert-Jaap Koops

Authors' backgrounds: Eleni Kosta is a legal researcher at the Interdisciplinary Centre for Law and Information & Communication Technology (ICRI) in the Katholieke Universiteit Leuven, and primarily works in the field of privacy and identity management, specialising on new technologies. Diana Bowman is a research fellow at the Institute for Energy and Environmental Law in the Katholieke Universiteit Leuven, working in the area of nanotechnology and regulation. Bert-Jaap Koops is professor of regulation & technology and Academic Director of the Tilburg Institute for Law, Technology, and Society (TILT) of Tilburg University, with a research interest in law & technology and other topics of technology regulation, such as information security, identity, and regulation of bio- and nanotechnologies.

The emergence of new technologies provides the potential for vast and varied applications, bringing with it both promise and peril. As Daniela Cerqui reminds us, technology has both good and bad implications, but its value does not depend merely on the uses to which it is put: technology is never neutral. Technology mirrors social and cultural values, if only because technology developers do not operate in a vacuum, but in a broader social and cultural context.

This dynamics of technology development and the socio-cultural context provides a relevant perspective for analysing a topical issue: the value of privacy in the up-coming era of converging technologies. Starting from the promises and perils of nanotechnologies, we will argue that the miniaturisation of technology, particularly through the combination of nanotechnologies, information and communication technology (ICT), and bio-implants, is likely to diminish the level of privacy protection in society, unless action is taken to actively embed privacy protection in technology. Cerqui argues that after the 'transplantation revolution', direct and unbounded sharing of information between a human being and their environment is possible but only if we discard privacy.[53] We will show that this is not necessarily the case: we can choose to retain at least a certain amount of privacy even in the

[53] Cerqui, D. (2007), 'An anthropological approach of technology and society: an overview'.

era of converging technologies, provided that it is embedded in the design stage of technology.

While the evolution of new technologies and applications, including the Internet and the World Wide Web, have fundamentally changed the way in which we, for example, communicate, work and even engage in everyday consumer transactions,[54] the borderless and ubiquitous nature of the 'Internet Revolution'[55] has similarly challenged society's ability to protect one's privacy. As the notion of privacy is not a static one, it is changing and adapting according to the needs of the society and the progress of technology. Data about the individual can be collected through various channels (for example see [Froomkin (2000)], such as cameras in public and private places, mobile phones, access cards, security controls or smart dust, to name just a few. The threats against privacy arising from Jeremy Bentham's conception of the 'Panopticon' or the ones described in the Orwellian society of 'Nineteen eighty-four' seem minimal compared to the mass threats against privacy posed by emerging technologies. At least in those societies, the individual had the knowledge that they could be being watched at any point in time. Baird and Vogt add to this that while "advances in information technology are already now augmenting concerns about privacy, […] these will be severely heightened by likely developments in nanotechnology" [Baird and Vogt (2004)].

Nanotechnologies and privacy

The nanotechnology 'revolution'[56] has already begun and as highlighted by Cerqui[57] in relation to all technologies, the coming 'nano-age' is likely to have both positive and negative impacts on society. Projected benefits of this heterogeneous family of technologies are anticipated across all industrial sectors including, for example, electronics, health, manufacturing and energy sectors.[58] At the same time, concerns have been raised over the

[54] See for example, United Nations Conference on Trade and Development (2004), *E-Commerce and Development Report 2004*, New York: United Nations; and United Nations Conference on Trade and Development (2005), *Information Economy Report 2005*, New York: United Nations.

[55] The phrase 'Internet Revolution' has been continually used within the literature. See for example: Bennahum, D.S. (1997), 'The Internet Revolution', *Wired*, 5(4), available at:

http://www.wired.com/wired/archive/5.04/ff_belgrad_pr.html; Litan, R.E. and A.M. Rivlin (2001), *The Economic Payoff from the Internet Revolution*, Washington DC: Brookings Institute Press; Giocannetti, E., M. Tsuji, and M. Kagami (2003), *The Internet Revolution: a Global Perspective*, Cambridge: Cambridge University Press; and Hillstrom, K. (2005), *Defining moment: the Internet revolution*, Detroit: Omnigraphics.

[56] Nanotechnology, the manipulation of matter at the atomic scale, exploits the fact that many nanosized materials display novel properties when compared to their macro or mircosized equivalents. Defined by its scale, a nanometer (nm) is one billionth (10^{-9}) of a meter, the platform technology conceptually refers to the ability to control the composition of molecules and atoms, within the range of 1.0-100nm (See for example: Woods, S., R. Jones and A. Geldart (2003), *The Social and Economic Challenges of Nanotechnology*, London: Economic and Social Research Council.)

[57] Cerqui, op. cit., n.53.

[58] Royal Society and Royal Academy of Engineering (2004), *Nanoscience and nanotechnologies: Opportunities and uncertainties*, London: RS-RAE.

potential health and safety implications of engineered nanoparticles,[59] and the impact of the emerging technology on privacy.[60]

While nanotechnology is still a relative young field of science, commentators have identified a range of potential products particularly within the field of 'nano-electronics' that may additionally challenge the current regulatory frameworks that are charged with protecting our privacy. These include the development of smart dust, 'ubiquitous miniature sensors floating around in the air'[61] designed to detect any communication information with other machines,[62] micro- or nano-scale Radio Frequency Identification (RFID) tags that could be incorporated into an extensive range of products for use in inventory control and products information storage purposes [Rodrigues (2006)], and the creation of nano-scale surveillance devices. In relation to the latter, Moor and Weckert suggest that it would make it 'extremely easy to put a nanoscale transmitter in a room or onto someone's clothing so that he or she will have no idea that the device is present or that he or she is being monitored and tracked....implanting tracking mechanisms within someone's body would also become easier with nanotech devices' [Moor and Weckert (2004)].

While the use of nano-scale monitoring and tracking equipment may pose a number of challenges to the protection of privacy, commentators such as Mehta[63] have also recognised that these developments may offer significant societal benefits within the fields of health care, environmental remediation and national security. Within the health-care sector for example, long-lasting nano-scale sensors designed to detect viruses, pathogens, and cancer cells may be embedded into the body to provide continuous health monitoring.[64] However, the use of nano-sensors and collection and use of sensitive health information including genetic information within this context may give rise to a number of potential privacy implications, as well as to other fundamental issues like employment and genetic discrimination. While these privacy and discrimination issues are far from unique to the advent of nanotechnology, there is the potential for these issues to be amplified by its invisible and unobtrusive nature.

Privacy in the era of converging technologies

Cerqui highlights the prospect of ICT convergence with cognitive sciences, noting for instance that, "information technologies are also getting closer to the human body with each

---

[59] See for example, [Oberdörster, *et al*. (2005)], [Lam, *et al*. (2006)], and Friends of the Earth (2006), *Nanomaterials, sunscreens and cosmetics: Small ingredients, big risks*, Sydney: FoE Australia and FoE United States.

[60] See for example, [MacDonald, (2000)]; Weckert, J. (forthcoming 2007), 'An approach to nanoethics', in Graeme Hodge, Diana Bowman, and Karinne Ludlow (eds), *New Global Regulatory Frontiers in Regulation: The Age of Nanotechnology*, Cheltenham: Edward Elgar.

[61] Froomkin (2000), p.1501.

[62] Pister, K. (2001), 'Smart dust: autonomous sensing and communication in a cubic millimetre', http://robotics.eecs.berkeley.edu/~pister/SmartDust/

[63] Mehta, M.D. (2002), 'Privacy vs Surveillance - How to avoid a nano-panoptic future', *Canadian Chemical News*, November-December, 31-33, at p.32.

[64] Royal Society and Royal Academy of Engineering (2004), *Nanoscience and nanotechnologies: Opportunities and uncertainties*, London: RS-RAE.

new breakthrough".[65] This is actually part of a longer-term development (10-20 years) of nanotechnologies' convergence with other technology platforms, specifically biotechnology and biomedicine, ICT and the cognitive sciences [Roco and Bainbridge (2002)]. This anticipated convergence has been labelled 'Nano-Bio-Info-Cogno', or NBIC. It is often associated with the idea of human enhancement or improvement, through for example, neuro-implants, cognitive enhancement, and brain-to-machine communication [Roco and Bainbridge (2002a)]. Should NBIC technologies be realised, Gordijn [Gordijn (2006)] argues that as with other technological developments, NBIC technologies will similarly bring with it promise and peril, highlighting the issue of infringement on privacy. Regardless of the trajectory of NBIC, it appears likely that the issue of privacy will remain as a central concern in the coming 'converging-technologies age'.

What role is there for privacy in this up-coming age? Technology is considered in several instances as privacy-destroying and is often perceived as a natural enemy of privacy.[66] No one can question the fact that an individual's privacy is threatened by the massive and easy collection of information realised through the use of emerging technologies. Notwithstanding the fact that new technologies have increased the amount of data collected, some believe that their actual sorting out and processing becomes even more cumbersome and costly. Contrary to the human processing that took place in the past, the one carried out by machines followed by human intervention for verification and checking can prove so expensive that many will not go on with it, "the costs of control [thus yielding] a certain kind of freedom".[67] This statement should of course be countered by the argument that the linking of available data or databases, data-mining, and profiling do allow an increasing scrutiny of groups and individuals, which may give substantially more power to law enforcement agencies and private companies over the individual. However, technology can work not only to the detriment of privacy but to its protection as well. Privacy Enhancing Technologies, such as P3P,[68] may assist individuals to secure themselves against technology violations and allow them to "enable upstream control of privacy rights as well as individual control."[69]

While considering the threats against privacy imposed by the broad use of nanotechnology, the French Data Protection Authority (CNIL)[70] highlighted that it shall be ensured by the European Data Protection Authorities that the wave of broad use of nanotechnologies "does not constitute a threat for the consistency of data protection principles and provisions, which are more relevant than ever".[71] CNIL seems however to forget in its thinking that new technologies create new expectations of privacy compared to the ones already existing. It is observed that when people interact in the on-line world, they are practically transferring their

---

[65] Cerqui, op. cit., n.53.

[66] Cerqui, op. cit., n.53: "But we cannot have both".

[67] Lessig L. (2006), *Code and other laws of cyberspace*, New York: Basic Books, at p.205

[68] The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents, for more information see http://www.w3.org/P3P/

[69] Lessig L. (2006), *Code and other laws of cyberspace*, New York: Basic Books, at p.231

[70] French Data Protection Authority (Commission nationale de l'informatique et des libertés)

[71] Communication presented by Philippe Lemoine and adopted on 12 January 2006 on *Nanotechnologies and data protection,* at p. 8

off-line expectations in this new environment. As mentioned by Leenes and Koops, "in the case of new, privacy invasive technologies, the user will have false expectation of privacy. And hence the use of such technologies will be considered a greater violation of privacy" [Leenes and Koops (2006)]. The reverse, however, is also true: as technology is slowly embedded in society, often to the detriment of privacy, reasonable expectations of privacy are lowered, resulting in a slow erosion of privacy through the mere development of technology. This process is hard to counter, but a conscious effort of society to stimulate and use PETs, notably in the design stage of technology, may provide a way to retain privacy after all. In order to continue to protect individual privacy, it is important that society anticipates the trajectory of developments within this field and takes a proactive approach to the implementation of relevant privacy safeguards. And while it is sometimes argued that privacy is rapidly becoming outdated, with younger generations caring less and less for keeping things private in the era of mobile communications, on-line communities, and Big Brother TV programs, it is not a foregone conclusion that privacy will not be considered an important value in future society. As De Hert and Gutwirth demonstrate, a democratic society needs both tools of transparency and tools of opacity, and privacy is a key tool of opacity to foster [Gutwirth and De Hert (2005)].

The vulnerability of privacy in light of all technology threats is beyond doubt. Maybe in the society of micro- and nano-technologies, of RFID chips and ICT implants, privacy has to be redefined. Machine-to-machine communication can lead the way for privacy-enhanced technology tools and new ways of communication, where the expectations of the individuals about privacy will differ from the ones they have had in earlier ages. But however changed, we believe that they will not disappear outright.

The important fact to bear in mind is that the relationship between technology and privacy is not intrinsically antagonistic. Although technology poses an abundance of new threats against privacy, it can also function as one of the means to protect privacy. Privacy-Enhancing Technologies have not found wide development or implementation yet, but that does not mean the promise of PETs will never come true. The best news is that slowly, technologies are emerging that incorporate privacy protection while at the same time allowing for other interests, such as security, ease-of-use, or efficiency.

As an example of these promising emerging technologies, we refer to information-security protocols being developed that reconcile information-sharing with confidentiality-keeping [Teepe (2006)]. These protocols allow interested parties, such as the police and national-security agencies, to have access to personal data and to compare these data with other databases, without actually being able to know the content of these data. This enables information-sharing and data-mining without infringing privacy up-front. Only after a match shows up, e.g., when a passenger on a flight to the United States features on the blacklist of people not allowed to enter the country, are the data of that particular passenger revealed to the proper authorities. As Wouter Teepe argues, not all privacy problems related to anti-terrorism measures can be solved by such protocols, but some of them can.[72] If 'privacy by design' is taken seriously, a new range of opportunities opens up. It is just a matter of deciding "what kind of society we want to live in, in the future".[73]

[72] Ibid., p. 176.

[73] Cerqui, op. cit., n.53.

Having these thoughts in mind we would like to believe that, despite all gloomy prognoses, 'all is not yet lost'.[74]

5.3 Reply 2: An anthropological approach of technology and society: an overview

Stefan Köpsell, TUD, Germany

Author's background: Stefan Köpsell is a researcher at the University of Technology Dresden.

In her statement Daniela Cerqui tries to explain and discuss the development of technologies and its impact on society and vice versa, using an anthropological approach and perspective. She presents "two classical visions of technology": technological neutralism and technological determinism. From the way it is presented, I got the impression that the usual way of understanding these terms is, that one has to decide which one of these two visions represents their own opinion and then stick to that decision. That means that one has to believe either in technological neutralism or determinism. Of course this strict categorisation does not make any sense. This is even realised by Daniela Cerqui, because she said that, "we find very often a mix of neutralism and determinism." This is not surprising at all. One simple explanation is that the term 'technology' is too wide. It covers too many concepts, mechanisms, things, visions and understandings making it impossible to just use one of these concepts to explain the impact of technology. If one really wants to decide if 'technological neutralism' or 'technological determinism' applies to a certain technology, one has to specify very carefully to which specific technology one refers to. General propositions about technology at large are always very questionable.

According to Cerqui, the 'technological determinism' can be further divided into '*technophile* determinism' (technology will offer the right solutions for our problems) and '*technophobe* determinism' (technology will lead us to a huge catastrophe). Again I got the impression that the usual way of thinking is, that one decides for one concept or the other. But I personally think that technology is at the moment the only feasible approach which offers (or has to offer and hopefully will offer) the right solutions for our problems - and, yes, it will lead us to a huge catastrophe. For me it is very similar to life in general, which finally always leads to a big catastrophe - namely: death. But does this imply that one should stop living?

Cerqui gives as an example for the mix of the concepts behind 'neutralism' and 'determinism' the "World Summit on the Information Society". She explained, that "most positions during the meetings assumed that we have no choice (determinism)". It stays unclear that 'no choice' means; no choice for or against what? Does it mean, that we have no choice that our society is heading towards what is called 'information society', does it mean that we have no choice how information is used or abused, does it mean that we have no choice that the 'information society' will lead us to a huge 'global digital divide'?[75] For all these possible 'no choice' options one can easily argue that we in fact have a choice - and moreover that technology is

[74] Froomkin (2000), p.1466.

[75] The 'digital divide' refers to the gap between people which are able to use all the modern (communication) technologies to access all the information available around the world and those which are not able to do this.

the enabling thing that gives us these choices. The 'use or abuse' of information can be influenced by privacy-enhancing technologies (i.e. by technologies which prevent or control the very existence of information) or by technologies related to digital rights management (i.e. technologies which control the usage of information); the 'digital divide' can be overcome by technologies which support the idea of open access to open content for everybody (like the "One Laptop per Child" initiative, free and open source software and the Internet itself etc.). Once again general statements with respect to 'choice' or 'no choice' related to a broad field of technologies like information and communication technologies do not seem to be very fruitful.[76] And the statement, explaining the position of the 'technological neutralism', which says that "we have to do the right things, if we want to reach the right goal" is so a general truth that any discussion is useless.

One of Cerqui's fundamental questions (or criticism, as I understand it) is the fact that people (or the society at large) tend to "take[…] for granted that technology does exist, and we 'just' have to assess it consequences". Inversion of her statement implies that she assumed that technology does *not* just exist. Before discussing if technology just exists or not, one has to clarify the meaning of the term 'exist' in this context. There are at least two different interpretations: 'exist' could refer to the awareness of the humankind for a certain technology, i.e. that people know how the technology works and prototypes and products for this technology do have a physical implementation. The other interpretation of 'exist' is a more metaphoric one: technology (or maybe more precise: the possibilities for and the concepts of a certain technology) 'exists' even without the existence of an individual, who is aware of this technology (i.e. knows about it). In this latter sense the 'development' or 'creation' of new technology will not really create something new (i.e. something which is not already there) - it is more a discovering process, i.e. a process which makes certain people or the public at large aware of that technology. So for instance for me the technology of a 'car' always existed, even if the concept was written down only some hundred years ago. Moreover even physical representations of technology may exist, even if nobody realises that it exists; just think of a stone which existed some billion years before the first humans used it as a tool or even as a weapon. All of our current technology is directly derived from the laws of nature. So if one believes that these laws of nature apply forever, i.e. without a beginning or an end, why should technology not exist in much the same way?

If one believes that technology 'just exists' then ethical or maybe anthropological issues related to the question, if one should 'develop' a certain technology or not, just melt down to the question, if on should make the public aware of certain technology. Now one can easily draw parallels to the discussion in the filed of ICT security. All of the ICT systems in use today have security holes and weaknesses. The main question is, if and how this should be made public. One party argues that security weaknesses have to be kept secret until the developers and operators have a chance to fix them; while the others argue that the security weaknesses should be published immediately to inform the public about the risks and to allow everybody to react accordingly. Applied to the field of technology the question arises, if one should develop (i.e. make the public aware of) a potentially harmful technology without knowing how to 'fix' it, or not? At least in the field of security it seems that it is widely agreed that 'security by obscurity' will lead to nothing than insecurity. But in the area of

[76] The possibility that there is in fact "no choice" because of some external third party which has control about every (human) being is not considered here because it would stop any disputation.

general technology the "avoiding technology (risks) by obscurity" approach seems to be widely adopted.

Summarising the said and responding to the statements from Daniela Cerqui: Yes, technology just exists and the only thing one can do is to assess its consequences. Doing this, the "avoiding technology (risks) by obscurity" does not seem to be very fruitful and will possibly lead to nothing but just a huge catastrophe.

Cerqui continues that "those who produce new technologies are at least as responsible as the users". I do not agree with this statement. I do not refuse a general responsibility of persons who make the general public aware of certain technology and make this technology available for them. But I do not agree that this person has more responsibilities than the person who actually uses the technology. This would make life much too easy for people who are not willing to take over responsibilities for their own life and what they are doing. Imagine for instance a murderer who argues that he is not solely responsible for what he has done, because the 'inventor' and producer of the knife are much more responsible for the homicide the murder has done.

Other interesting questions Cerqui poses are: "What we develop these technologies for? What is the ultimate goal? Why do we want them? What implicit project for society and humankind are they part of?" Especially the third question "Why do we want them?" implies that the main goal of developing technology is to have them after the developing has finished successfully. But to my understanding this is not always the ultimate goal of developing new technologies. In many cases it seems that "the way is the goal", i.e. that technology is developed just because we can or we want to find out if we can or not. So the ultimate goal is the process not the product. Whether a certain technology is useful or not does not matter. Moreover it is very often impossible to predict, if a certain development would be useful or not. There exist many examples, where inventions of the paste reveal there whole potential only in our days.

Cerqui said that "our western society has clearly chosen a technologically mediated way of living." I just want to question, how we 'chose' this technologically mediated way of living? Was it an informed decision, a silent agreement, some kind of consensus? Or did we in the end not really 'chose' this way of living - because what we did was just not to vote against it?

Cerqui also stated that "we are convinced that there is no other option" (with respect to the technologically mediated way of living). At least I am not convinced and I also do not want to spread it all over the world. I just see the "technologically mediated way of living" as one option of how to live - and it is an option I like.

Cerqui draws the conclusion that in our new 'information society' the keyword for success is: access. "And the quicker access, the better." Even so 'access' might be a precondition for being successful in an 'information society', but it is by no means the central point. The central point might be processing of information and gaining useful knowledge. I do not see a clear relation between 'access to information' and 'gaining of knowledge'. Especially one does not imply the other. For me it is questionable if getting access to more and more information in an ever faster way will really lead to more useful knowledge and those successes. Moreover it seems more realistic that the over stimulation with information will hide any useful knowledge. So probably not the one who has the most information but the one who has the fewest will be successful. Applied to our today's situation this means that not the one who gets the most SPAM is the successful one, but the one who has the best SPAM filter.

Another way of reasoning about the success in the information society is the amount of attention one can get from others. The more attention one is able to get from others, the more successful one would be in the information society. And this has already started: just look at Google, You Tube or Second Life.

Cerqui then cited Virilio. According to him "the history of humankind has seen three major revolutions that points towards an ever-increasing speed in getting in touch with the world. The first one – in transportation, [..] the second revolution – that of transmission or communication [..] and the third revolution – that of transplantation [..]." For me this looks much like the typical naive approaches of "creating fancy looking categories by three minute thinking". Especially the relationship between the first and the second one is very questionable, because it says that communication allows things to be done faster compared to the case where one would be required to move oneself. But what if techniques like teleportation, materialisation or similar techniques become reality one day? In this case the distinction made above is not true anymore. Also I can not really see the relation of the third 'revolution' with the other ones.

When it comes to privacy and information technology Cerqui argued that "IT must by definition be transparent" and that "we cannot have both": free flow of information and privacy. The assumption that "IT must be transparent" is probably one of the biggest ICT related misconceptions. Of course ICT has to be designed in a usable and accessible way. But this does by no means imply that ICT has to be 'transparent'. Moreover in many cases 'transparency' is contradictory to usability. Just to give an example of that I mean: If we look at cars then clearly a car user does not need to know all the details about how the car is working. Nevertheless he needs to have some basic understanding of the overall functionality, i.e. he needs to know the very basics about the functionality of the engine. Otherwise (in case of 'technology transparency') it would be very hard to 'teach' the user that he has to drive from time to time to obscure looking buildings, where he has to put in some strange looking device into his care. I am quite sure that in case of 'technology transparency' dozens of non working cars will lay on the edge of the road, just because they are out of fuel. Applying this to ICT it means, that we should not go for 'total transparency' but instead should teach the people the necessary basics of the ICT functionality and this way make them aware of potential problems.

Regarding the question, if "we cannot have both of them", one has to say that the distinction between "the information must circulate without any boundaries and everybody can access everything in real time" and "our privacy to be preserved" is much too much black and white. There are many shades of grey in between. First of all not everybody needs access to every information all the time without any boundaries. One simply has to carefully design and decide who needs access to which information, for which purpose, for how long etc. The development of privacy-enhancing technologies will enable to implement decisions.

Summarising the said, we always have a choice in which direction our society wants to go, technology will support our decisions and technicians should design the new technologies in a way that these new technologies are intrinsically more good than bad.

5.4 Reply 3: An anthropological approach of technology and society: an overview

Martin Meints

Author's background: Martin Meints is a scientific researcher and security auditor at the Independent Centre for Privacy (ICPP) of Schleswig-Holstein, Germany.

Cerqui introduces the theories of technology determinism and technology neutralism. In her analysis she comes to the conclusion that technology is never neutral, but also not deterministic. Analysing the relationship between modern western societies and technology she comes to the conclusion, that the adaptation and use of technologies is an important part of these societies and thus evasion of technologies by individual members of theses societies becomes difficult. She further concludes that the future information society using ICT implants will also lead to a society that will be transparent for any flow of information. As IT has to be transparent by default, we can either opt for free flow of information, or privacy.

Society knows different types of research. The most relevant two of them can be classified as (a) clearly target-oriented research and (b) as fundamental research. While target-oriented research aims at research results with a clear purpose of use or even a market in mind, fundamental research aims at methods, mechanisms or components that can be used in many ways and for many purposes. Research projects clearly seem to belong to one of these classes. But history shows that research projects may change their class or split up in two or more tracks. One example for this is research in nuclear fission – it started as fundamental research and led to nuclear power stations and atomic bombs.[77] The risk of radioactive contamination is well known, taken into consideration and "managed". Another example is the development of Thalidomide sold as Contergan, a pharmaceutical substance planned to be used as pain killer. Unfortunately Contergan caused birth deformities, notably in Germany in the early 1960s. Contergan consequently as pain killer was removed from the market. Today Contergan is back in the market – it meanwhile showed to be one of the most efficient medicines against leprosy, despite the well known adverse effects.[78]

Both examples show that technology is neither deterministic, nor neutral. In addition these examples show that society can make a choice how technology is being implemented and used, taking adverse effects into consideration. Technology and risk assessment and as a result modification of the implementation or the technology itself and in some cases even the decision not to use the technology are well possible (see e.g. regulations for security of products and the prohibition of certain drugs). Regulations on the implementation and use of technology in many cases come along with law enforcement, typically by police and justice. Society in the past proved well to be able to manage technologies and their use.

Cerqui points out that access to information is the keyword to understand the driving force of the information society. She also points out that the speed one is able to access the information is important. But quality of the information also is a relevant aspect not mentioned as such by Cerqui, though the ability to access information timely is clearly an aspect of quality. Another relevant aspect of quality is context-dependence –information not related to the context one is interested in is just noise and consumes brain resources without

[77] See e.g. http://en.wikipedia.org/wiki/Nuclear_fission

[78] See e.g. http://en.wikipedia.org/wiki/Thalidomide

any benefit or may even lead to wrong decisions. Though context related technologies such as data mining that made impressive progress, context detection, context linking and context verification still requires quite some know-how and effort.

Another aspect that seems important is that IT is not transparent by default. First of all, IT is very complex and nowadays complexity increases further. As a result even experts do not understand all aspects of today's integrated IT systems. In this context trustworthiness of hard- and software modules and components, based on standardised evaluation procedures e.g. carried out by trusted third parties, becomes important. Secondly research in IT security (today also called information security) already is dealing among others with confidentiality of information processed by IT systems.[79] As a result in most cases there is no free flow of information in IT systems today. Information typically is used in communicational contexts. It may well move from one context to another, but there are areas e.g. in military research, planning and operations, where information is efficiently kept secret. In addition the transfer of personal data from one context (e.g. the original purpose for which the data have been collected and processed) to another one is in Europe regulated by data protection legislation. Legislation and market forces (e.g. trade secrets) together with information security mechanisms provide for important domains of opacity.

Opacity in many cases is a result of information asymmetry. Information asymmetry of course may have negative effects such as 'lemon markets' (Akerlof 1970) and building of monopolies. In cases where society is not willing to accept these monopolies, we soon observe regulatory approaches, for example at the moment at European market for electric energy.[80]

It is difficult to predict what the results from ICT implants such as body to system or brain to brain communication may look like. The human nerve system is not readily understood yet, and scientists only have a rough idea how the human brain works.[81] Free and transparent flow of information will depend on the type of ICT implant and it position, determining the way to access the brain. In addition the brain will adapt to the implant and the resulting flow of information. And it is very possible that certain types of ICT implants show severe adverse effects in a similar way, we know this from pharmaceuticals.

From my personal point of view a positive and constructive use of ICT implants today seems possible. Probably we will see limitations in purposes of implantation, types of implants and places where implants are allowed to further guarantee the existence of domains of opacity. Filters controlled and configured by the bearer of the implant might be a future Privacy Enhancing Technology (PET) in this context.

The most relevant aspect to me seems where the borders between the domains of transparency and opacity are and who controls them. Who acts in which informational context on which side of the border primarily is a question of power, as outlined by Hildebrandt and Gutwirth [Hildebrandt, Gutwirth and de Hert, 2005] when analysing constitutional democracies.

---

[79] As a result a number of international standards emerged, such as ISO 27001, ISO 17799, CobiT and others.

[80] See e.g. http://www.atkearney.de/content/misc/wrapper.php/name/file_pdf_strommarktliberalisierung_secure_11764683247e0c%5B1%5D_1177488973d8c1.pdf

[81] See for example some of the articles in http://www.zeit.de/wissen/hirnforschung/hirnforschung_schwerpunkt

5.5 An anthropological approach of technology and society: a final riposte

Daniela Cerqui

It is true that technology is a wide phenomenon. It is also true that an important part of anthropology is dedicated to the study of the relationship human beings develop with technology, considered as a natural human attribute. Several famous anthropologists and palaeontologists have studied the history of humankind, and have shown that there have been no human beings without technology (see for instance [Leroi-Gourhan, (1964, 1965)]). Therefore, general propositions about technology are necessary to understand its universal aspect and what it means for us, as humans. Then, this has to be considered in comparison with specific manifestations: technologies can be understood in their cultural dimension. The main goal of a committed anthropological approach applied to technology is to make people aware that it is never neutral, and that there are values embedded in it. It seems that such a statement can lead to a few misunderstandings.

First, this does not mean that the user is not responsible for his/her use, as suggested by Köpsell, in reply 2. On the contrary, our legal system is based on the responsibility of the user, and it is a good pragmatic approach. But one should be sensitive to the different levels of analysis, as there is also a deeper level, which is the one we forget when focusing on the user. Generally speaking, responsibility does not start once the device is produced. Thinking that technology is the only feasible approach to solve our problems is a cultural vision of the world. Reply 2 is a very typical example of a speech that does not stand back from its own values at all: the difference between a stone used as a weapon and a technological weapon is that the second one was built by people, according to a clear project. There is also one big common denominator: in both cases we should not just think about how to use the object, but about which values are behind this use.

The aim of anthropology is not to promote 'good' technologies, but to show that there is always a dark side included in the package. If we want the bright side, we have to cope with the dark one. And until we consider it simply as a side effect, we cannot face it properly. Wise political reflection has to take that into account.

For instance, the idea that technology can work not only to the detriment of privacy but also to its protection[82] is a very good starting point for acting based on an anthropological standpoint. Such a position admits the two faces of the coin. When describing privacy as a dynamic notion, it implies that privacy might have to be redefined because new expectations appear, and it can definitely lead us to think about how to balance good and bad impact.

The more information circulates, the better we understand that it needs boundaries. It is true, as argued by Meints in reply 3, that IT are not transparent in the way they work. Nevertheless, my point is not about the way they work, but about what they are supposed to bring to the user, whose access is supposed to be unlimited to data. In such a context, making the machines 'userfriendly' is one more way to make sure you do not loose time understanding how it works and you can directly become an efficient user.

[82] As developed by Kosta, Bowman and Koops in reply 1.

Information security is a very good illustration of how sometimes we try to give limits afterwards to a system which was first built to have insufficient boundaries. It does not make sense to create new ways for keeping information secret, every time we realise that there is a new 'sensitive' field in which unlimited access may be a problem. That is a reactive way of acting, based on a misunderstanding of the fundamental logic. Focusing on these boundaries just gives us the illusion that we master the flow and the way it is oriented, but we do not, unless we develop an anticipative reflex, taking into account the various plausible scenarios for the future.

That implies an interdisciplinary collaboration, involving people open-minded enough to be embracing of other points of view. But respect for other scientific fields may well be an unreachable goal for some (disagreement is one thing, contempt is another!), therefore, the road is still long.

6 Conclusion

Undeniably we have adopted a technologically mediated way of living. This has come to such a degree that technology pervades every aspect of our lives. It is perhaps because we are becoming more and more reliant on technology that we are coming to appreciate that traditional interfaces underexploit the processing potential of both the user and technology. In essence this occurs because of a bottleneck in the link between thinking what we want to happen, and laboriously pursuing those actions. Indeed, the fundamental issue can be viewed as two powerful information processors (human and machine) attempting to communicate with each other via a narrow bandwidth, highly constrained interface. Given this, it is unsurprising that the concept of AmI is so appealing – shift the onus onto the technology to know what we want and when we want it rather than us needing to use the technology as a tool to pursue it. Indeed maybe even allow the environment to make decisions for us, or offer us services that perhaps we did not even know we wanted.

The technical issues relating to the actual implementation and thus realisation of Ambient Intelligence (AmI) environments are immense, and in most cases tangible solutions to technical related problems are still yet to be found. This situation leads to some interesting points of debate on technical, legal and wider societal levels. The concept of AmI is largely based on the idea that by augmenting an environment with sensor technologies and by providing near unlimited storage and processing capabilities, the intentions, needs and desires of people can be predicted and catered for. The result is that people will not need to know how to operate complex technologies – instead the technology will interact with them in intelligent and intuitive ways. Clearly collating information is the key. However, if an environment is to know what a person wants or needs without being explicitly told, then this information needs to come from indirect means – i.e. the technology, or rather the environment as a whole becomes less interactive, and more proactive. Through varying levels of sensor data gleaned from pervasively embedded sensors, dynamic autonomic profiles can be drawn to enable this proactive ability. Intuitively these profiles can only be as good as the data that feeds them, and the processing available to create them, and hence the focus of development is to extract as much data as possible from all aspects of the users and their interactions within an AmI space, as well as developing the underlying infrastructure through which this data can be 'mined' for new information. 'Emerging Technologies' has become a term which considers the convergence of areas such as nanotechnology, biotechnology, information technology, cognitive science, robotics, and artificial intelligence. As discussed here, such technologies which stem from this idea of domain fusion can be considered appropriate in the fabric of an AmI environment, meaning that AmI may actually be an application area made possible through this new emerging technology phenomenon. However, as with all technology, there is clearly a price to pay. Such capabilities come at a cost to our privacy and can clearly start to ebb away our fundamental human rights.

This deliverable is not about finding firm answers to specific questions - indeed to a large extent it would be too presumptuous to do so. Instead it aims to inform the reader and most importantly to stimulate further discussion on both the specific and broader issues that such development entails. In essence, there are more questions posed than answers given. However, perhaps the most important point is: who is going to address the questions raised here, when, and how?

7 References

Akerlof, G. A., 'The Market for 'Lemons': Quality Uncertainty and the Market Mechanism', *Quarterly Journal of Economics* 84 (3): 488-500.

Allen, G., Goodale, T., Russell, M., Seidel, E., Shalf, J. (2003), 'Classifying and enabling Grid applications', in *Grid Computing – Making the Global Infrastructure a Reality*, John Wiley & Sons.

Baird, D. and T. Vogt (2004), 'Societal and Ethical Interactions with Nanotechnology ('SEIN') – An Introduction', *Nanotechnology Law & Business,* 1(4), 391-396.

Bell, D. (1973) 'The Coming of Post-Industrial Society: a Venture in Social Forecasting', Basic Books, New York.

Bell, D. (1999) 'The axial age of technology', Foreward: 1999, The Coming of Post-Industrial Society. Basic Books, New York.

Berka, C., Levendowski, D.J., Cvetinovic, M., Petrovic, M. M., Davis, G. F., Lumicao, M. N., Popovic, M. V., Zikovic, V. T., Olmmstead, R. E. (2004), 'Real-time analysis of EEG indices of alertness, cognition and memory acquired with a wireless EEG headset', *International Journal of Human-Computer Interaction, 17*, pp. 151-170.

Berman, F., Hey, A., Fox, G. (2003), 'The Grid: past, present, future', in *Grid Computing – Making the Global Infrastructure a Reality*, John Wiley & Sons.

Bizer, J, Spiekermann, S., Günther, O. (2006), 'Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS)', Berlin 2006.

Borcea, K., Donker, H., Franz, E., Liesebach, K., Pfitzmann, A., Wahrig, H. (2005), 'Intra-application partitioning of personal data'. *In Proc. of PEP*, Edinburgh, UK, pp. 67–74.

Borcea-Pfitzmann, K., Liesebach, K., Pfitzmann, A. (2005), 'Establishing a privacy aware collaborative eLearning environment', *In Proc. of EADTU 2005*, Rome.

Bozorgzadeh, Z., Mason, S. G., Birch, G. E. (2000), 'The LF-ASD BCI: On-line identification of imagined finger movements in spontaneous EEG with able-bodied subjects', *Proc. IEEE Int. Conference on Acoustics, Speech and Signal Processing*, Istanbul, Turkey.

Chapin, J. K., Moxon, K. A., Markowitz, R. S., Nicolelis, M. A. (1999), 'Real-time control of a robot arm using simultaneously recorded neurons in the motor cortex', *Nature Neuroscience, 2*, 1999, pp. 664-70.

Cohen L. G., Celnik, P., Pascual-Leone, A., Corwell, B., Falz, L., Dambrosia, J., Honda, M., Sadato, N., Gerloff, C., Catala, M. D., Hallett, M. (1997), 'Functional relevance of cross-modal plasticity in blind humans', *Nature, 389*, pp. 180-83.

Cohen, M., Herder, J., Martens, W. L. (1999), 'Cyberspatial audio technology', *JAESJ, J. Acoustical Society of Japan (English), 20(6)*, November, 1999, pp. 389-95.

Dertouzos, M. (1997) 'What will be. How the world of information will change our lives'. Harper, San Franciso.

Dobelle, W. H. (2000), 'Artificial vision for the blind by connecting a television camera to the visual cortex', *ASAIO J., 46*, pp. 3-9.

Donoghue, J. P. (2002), 'Connecting cortex to machines: Recent advances in brain interfaces', *Nature Neuroscience, Vol. 5 Supplement*, pp. 1085-88.

Edward Elgar; and Rodrigues, R. (2006), 'The Implications of High-Rate Nanomanufacturing on Society and Personal Privacy', *Bulletin of Science, Technology & Society*, 26(1), pp. 38-45.

EGE (The European Group on Ethics in Science and New Technologies) (2005), 'Ethical Aspects of ICT Implants in the Human Body', Adopted on 16 March 2003, available at ec.europa.eu/european_group_ethics/docs/avis20_en.pdf.

Foster, I. (2002), 'What is the Grid? A Three Point Checklist', *GRID Today*, July 20th, 2002.

Foster, I. (2006), 'Globus Toolkit Version 4: Software for Service-Oriented Systems', *IFIP International Conference on Network and Parallel Computing*, Springer-Verlag, LNCS 3779, pp. 2-13.

Foster, I., Kesselman, C., Tuecke, S., (2001), 'The Anatomy of the Grid: Enabling Scalable Virtual Organizations', Intl J. Supercomputer Applications, 15(3).

Foster, I., Kishimoto, H. 'The Open Grid Services Architecture, Version 1.5'.

Franz, E. and Engel, B. (2006), 'A realization of context management facilitating the usage of partial identities', *In Proc. of PEP*, Edinburgh, UK, pp. 23–28.

Franz, E., Liesebach, K., Borcea-Pfitzmann, K. (2006a), 'Privacy-aware user interfaces within collaborative environments', *In Workshop on Contexts in Advanced Interfaces at AVI 2006*, Venice, Italy.

Franz, E., Springer, T., Dargie, W. (2007), 'The May Faces of Context', *submitted to: CASEMANS 2007, Int. Workshop on Context-Awareness for Self-Managing Systems* (Devices, Applications and Networks), Toronto, Canada.

Froomkin, A.M. (2000), 'The death of privacy?', *Stanford Law Review*, 52, pp. 1461-1543.

Garreau, J., (2004) *Radical Evolutio*n: The promise and peril of enhancing our minds, our bodies-and what it means to be human. New York: Doubleday, pp. 78-79.

Gasson, M.N., Hutt, B.D., Goodhew, I., Kyberd, P., and Warwick, K. (2005), 'Invasive Neural Prosthesis for Neural Signal Detection and Nerve Stimulation', *International Journal of Adaptive Control and Signal Processing*, Vol.19:5, pp. 365-75.

Gasson, M.N., Wang, S.Y., Aziz, T.Z., Stein, J.F., Warwick, K. (2005b), 'Towards a Demand Driven Deep-Brain Stimulator for the Treatment of Movement Disorders', *MASP2005, 3rd IEE International Seminar on Medical Applications of Signal Processing*, London, UK, pp. 83-86, 3-4 November, 2005.

Gates, B. (1996) 'The Road Ahead'. Penguin, London.

Gordijn, B. (2006), 'Converging NBIC Technologies for Improving Human Performance: A Critical Assessment of the Novelty and the Prospects of the Project', *The Journal of Law, Medicine & Ethics*, 34(4), pp. 726-732.

Grimm, C., Pattloch, M., Reiser, H. (2006), 'Sicherheit in Grids', *PIK Praxis der Informationsverarbeitung und Kommunikation*, K.G. Saur Verlag, Issue 3, July-September 2006, pp. 159-165.

Gutwirth, S. and P. De Hert (2005), 'Privacy and Data Protection in a Democratic Constitutional State', in: Hildebrandt, M. and S. Gutwirth (eds.), *Implications of profiling practices on democracy and rule of law*, FIDIS Deliverable D7.4, available at http://www.fidis.net, pp. 11-28 at p. 24.

Gutwirth, S., (1993), *Waarheidsaanspraken in recht en wetenschap [Claims on Truth in Law and Science]*, Brussel, VUBPRESS, 846 pp. 34-35.

Hildebrandt, M., Gutwirth, S., de Hert, P., (2005) FIDIS Deliverable - D7.4: Implications of profiling practices on democracy and rule of law, Frankfurt a.M. Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.4.implication_profiling_practices.pdf

Hoffknecht, A., Teichert, O., (2006), 'Nutzung der Nanotechnologie für sicherheitstechnische Anwendungen', *Zukünftige Technologien Nr. 63*, VDI Technologiezentrum, Berlin 2006.

Humphrey, M., Thompson, M., (2003) 'Security Implications of Typical Grid Computing Usage Scenarios', *OGF Document GFD.12.*

James, C. J., Gibson, O. J. (2003), 'Temporally constrained ICA: an application to artifact rejection in electromagnetic brain signal analysis', *IEEE Trans. Bio. Eng., 50(9)*, pp. 1108-16.

Jennings, N., Wooldridge, M., (1996) 'Software Agents', *IEE Review*, pp. 17-20.

Kennedy, P., Andreasen, D., Ehirim, P., King, B., Kirby, T., Mao, H., Moore, M. (2004), 'Using human extra-cortical local field potentials to control a switch', *J. Neural Eng., 1*, pp. 72-77.

Kubler, A., Kotchoubey, B., Hinterberger, T., Ghanayim, N., Perelmonter, J., Schauer, M., Fritsch, C., Taub, E., Birbaumer, N. (1999), 'The Thought Translation device: a neurophysiological approach to communication in total motor paralysis', *Experimental Brain Research, 124*, pp. 223-32.

Lam, C. *et al*. (2006), 'A Review of Carbon Nanotube Toxicity and Assessment of Potential Occupational and Environmental Risks', *Critical Reviews in Toxicology*, 36, pp. 189-217.

Leenes, R.E. and B.J. Koops (2006), ''Code' and privacy or how technology is slowly eroding privacy', in E. Dommering and L. Asscher (eds), *Coding Regulation: Essays on the Normative Role of Information Technology* (Information Technology and Law Series, 12), Den Haag: T.M.C. Asser Press, pp. 141-203.

Leroi-Gourhan, André, 1964, *Le geste et la parole I. Technique et langage*. Paris: Albin Michel.

Leroi-Gourhan, André, 1965, *Le geste et la parole II. La mémoire et les rythmes.* Paris : Albin Michel.

Lieberman, H., Selker, T. (2000), 'Out of context: Computer systems that adapt to, and learn from, context', *IBM Systems Journal*, 39(3&4), pp. 617.

Lisetti, C., Nasoz, F. (2004), 'Using Non-invasive Wearable Computers to Recognize Human Emotions from Physiological Signals', J. Applied Signal Processing 11, pp. 1672-87.

Litke, A., Skoutas D., Varvarigou T. (2004), 'Mobile Grid Computing: Changes and Challenges of Resource Management in a Mobile Grid Environment', presented in Workshop: "Access to Knowledge through Grid in a Mobile World", PAKM 2004 Conference, Vienna.

Liu, W., Sivaprakasam, M., Singh, P. R., Bashirullah, R., Wang, G. (2003), 'Electronic visual prosthesis', *Artificial Organs, 27(11)*, pp. 986-95.

Lusted, H. S., Knapp, R. B. (1996), 'Controlling computers with neural signals', *Scientific American, 275(10)*, pp. 58-63.

MacDonald, C. (2000), 'Nanotechnology, privacy and shifting social conventions', *Health Law Journal*, 12, pp. 37-40

Chetty, M., Buyya, R. (2002), 'Weaving Computational Grids: How Analogous Are They with Electrical Grids?', *Computing in Science and Engineering, 4(4)*, pp. 61-71.

Mann, S. (1997), 'Wearable Computing: A first step towards personal imaging', *IEEE Computer, 30(2)*, pp. 25-32.

McCabe B. F. (1979), 'Autoimmune sensorineural hearing loss', *Ann. Otol. Rhinol. Laryngol., 88(5-1)*, pp. 585-9.

McCloskey, P., Delaney, K., Barton, J., Mahmood, R.K., O'Mathuna, C., Duffy, G. (2004) 'From RFID to Smart Dust: a perception of future applications', Smart Wireless Tags Workshop, Brussels.

Meijer, P. B. L. (1992), 'An experimental system for auditory image representations', *IEEE Trans. Bio. Eng., 39(2)*, pp. 112-21.

Millan, Jd. R., Renkens, F., Mourino, J., Gerstner, W. (2004), 'Noninvasive brain-actuated control of a mobile robot by human EEG', *IEEE Trans. Bio Eng., 51(6)*, pp. 1026-33.

Moor, J. and J. Weckert (2004), 'Nanoethics: Assessing the Nanoscale from an Ethical Point of View', in D. Baird, A. Nordmann, and J. Schummer (eds), *Discovering the Nanoscale*, Amsterdam: IOS Press, pp. 301-310.

Nicolaou, N., Nasuto, S. J. (2003), 'Comparison of temporal and traditional Independent Component Analysis (ICA) algorithms for EEG analysis', *Proc. of ICANN/ICONIP'03, Joint 13th International Conference on Artificial Neural Networks and 10th International Conference on Neural Information Processing*, Istanbul, Turkey, June 26-29, pp. 157-60.

Nwana, H. S., 'Software Agents: An Overview', *Knowledge Engineering Review*, Vol. 11, No 3, pp. 1-40, September 1996. Download:
http://www.sce.carleton.ca/netmanage/docs/AgentsOverview/ao.html

Oberdörster, G., *et al*. (2005), 'Review: Principles for characterizing the potential human health effects from exposure to nanomaterials: elements of a screening strategy', *Particle and Fibre Toxicology*, 2(8), pp. 1-35.

Pankanti, S, Bolle, R.M., and Jain, A., (2000), 'Biometrics: The Future of Identification,' *Special Issue of IEEE Computer on Biometrics*, pp. 46-49.

Paschen, H., Coenen, C., Fleischer, T., Grünwald, R., Oertel, D., Revermann, C. (2004), *Nanotechnologie*, Springer-Verlag, Heidelberg.

Penny, W. D., Roberts, S. J., Everson, R. M. (2000), 'Hidden Markov Independent Components for biosignal analysis', *Proceedings of MEDSIP-2000, Int. Conf. on Advances in Medical Signal and Information Processing*.

Pfurtscheller, G., Muller, G. R., Pfurtscheller, J., Gerner, H., J., Rupp, R. (2003), 'Thought control of functional electrical stimulation to restore hand grasp in a patient with tetraplegia', *Neurosci. Lett., 351(1)*, pp. 33-36.

Radoykov, B., Rundle M., Conley, C. (2007) 'Ethical Implications of Emerging Technologies: A Survey', Paris, Unesco, 92 http://unesdoc.unesco.org/images/0014/001499/149992E.pdf

Ravi, K. V. R., Palaniappan, R., (2005), 'Recognising Individuals Using Their Brain Patterns', *ICITA (2) 2005*, pp. 520-523.

Richta, R. (1969) 'La civilisation au carrefour'. Anthropos, Paris.

Riva, G., Loreti, P., Lunghi, M., Vatalaro, F. & Davide, F. (2003) '4. Presence 2010: The Emergence of Ambient Intelligence' in Riva, G., Davide, F., Ijsselsteijn, W.A. (Eds.), *Being There: Concepts, effects and measurement of user presence in synthetic environments*, Amsterdam: IOS Press.

Rizzo, J. F., Wyatt, J., Humayun, M., DeJuan, E., Liu, W., Chow, A., Eckmiller, R., Zrenner, E., Yagi, T., Abrams, G. (2001), 'Retinal Prosthesis: An Encouraging First Decade with Major Challenges Ahead', *Editorial, Ophthalmology, 108(1)*, pp. 13-4.

Roco, M.C. and W.S. Bainbridge (2002), 'Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science', Arlington, Virginia: National Science Foundation.

Roco, M.C. and W.S. Bainbridge (2002a), 'Converging technologies for improving human performance: Integrating from the nanoscale', *Journal of Nanoparticle Research*, 4, pp. 281-295.

Romo, R., Hernandez, A., Zainos, A., Brody, C. D., Lemus, L. (2000), 'Sensing without touching: psychophysical performance based on cortical microstimulation', *Neuron, 26*, pp. 273-78.

Satyanarayanan, M. (2005), 'Energy Harvesting & Conservation', *IEEE Pervasive Computing*, Vol. 4, No. 1, January-March 2005.

Schmidt, A., Beigl, M., Gellersen, H.W. (1999), 'There is more to context than location', *Computer and Graphics*, 23(6), pp. 893–901.

Schmorrow, D., & McBride, D. (2004), 'Introduction. Special issue on Augmented Cognition', *International Journal of Human-Computer Interaction*, 17(2), pp. 127-130.

See Doyere, V., Debiec, J., Monfils, M-H., Schafe, G.E., Ledoux, J., 'Synapse-specific reconsolidation of distinct fear memories in the lateral amygdala', Nature Neuroscience, March 2007, pp. 414-416.

Shimojo, S., Shams, L. (2001), 'Sensory modalities are not separate modalities: plasticity and interactions', *Current Opinion in Neurobiology, 11*, pp. 505-09.

Shneiderman, B. (2000), 'The limits of speech recognition', *Communications of the ACM, 43(9)*, pp. 63-65.

Steel, D., 'Smart Dust', *University of Houston ISRC Technology Report*, Houston, March 2005. Available at http://www.uhisrc.com/FTB/Smart%20Dust/Smart%20Dust.pdf

Streitz & Nixon (2005), 'The Disappearing Computer', *Communications of the ACM*, Vol. 48 (3), March 2005. pp. 33-35.

Sykacek, P., Roberts S., Stokes, M. (2004), 'Adaptive BCI based on variational Bayesian Kalman filtering: an empirical evaluation', *IEEE Trans. Bio. Eng., 51(5)*, pp. 719-29.

Talwar, S. K., Xu, S., Hawley, E. S., Weiss., S. A., Moxon, K. A., Chapin, J. K. (2002), 'Rat navigation guided by remote control', *Nature, 417*, pp. 37-38.

Thorpe, J., van Oorschot, P. C., and Somayaji, A., (2004), 'Pass-thoughts: Authenticating With Our Minds', *In Proceedings of the ACSA 2005 New Security Paradigms Workshop*, Sept. 2005, Lake Arrowhead, California, USA, pp. 45-56.

Tufte, E. R. (1989), 'Visual design of the user interface', IBM Corporation, Armonk, N.Y.

Turk, M. (2000), 'Perceptive media: machine perception and human computer interaction' *Chinese Journal of Computers, 23(12)*, pp. 1235-44.

Uludag, U. and Jain, A. K. (2004), 'Attacks on biometric systems: a case study in fingerprints', *Proc. SPIE-EI 2004*, pp. 622-33, San Jose, CA, January 18-22.

Virilio, P. (1995) La vitesse de libération. Galilée, Paris.

Warwick, K., Gasson, M. (2004a), 'Extending the Human Nervous System Through Internet Implants - Experimentation and Impact', *IEEE SMC, IEEE International Conference on Systems, Man and Cybernetics*, The Hague, The Netherlands, pp. 2046-52, 10-13 October.

Warwick, K., Gasson, M., Hutt, B., Goodhew, I., Kyberd, P., Schulzrinne, H., Wu, X. (2004b), 'Thought Communication and Control: A First Step Using Radiotelegraphy', *IEE Proc. Communications*, Vol.151:3, pp. 185-89.

Warwick, K., Gasson, M.N., Hutt, B.D., Goodhew, I. (2005), 'An Attempt to Extend Human Sensory Capabilities by Means of Implant Technology', *IEEE SMC, IEEE International Conference on Systems, Man and Cybernetics*, Waikoloa, Hawaii, pp. 1663-68, 10-12 October.

Warwick, K., Gasson, M.N., Hutt, B.D., Goodhew, I., Kyberd, P., Andrews, B.J., Teddy, P., and Shad, A. (2003) 'The Application of Implant Technology in Cybernetic Systems', *Archives of Neurology, Vol.60(5)*, pp. 1369-73.

Welch, V. Siebenlist, F. Foster, I. Bresnahan, J. Czajkowski, K. Gawor, J. Kesselman, C. Meder, S. Pearlman, L. Tuecke, S. (2003) 'Security for Grid Services', Twelfth International Symposium on High Performance Distributed Computing (HPDC-12), pp. 48-57.

Welen, P., Wilson, A., Nixon, P. (2003) 'Scenario Analysis', Gloss Deliverable D.9., http://iihm.imag.fr/projects/Gloss/Deliverables/D9-1.pdf.

Wessberg, J., Stambaugh, C. R., Kralik, J. D., Beck, P. D., Laubach, M., Chapin, J. K., Kim, J., Biggs, S. J., Srinivasan, M. A., Nicolelis, M. A. (2000), 'Real-time prediction of hand trajectory by ensembles of cortical neurons in primates', *Nature, 408*, pp. 361-65.

Winter, R., Burns, R. (2006), 'Managing Data Warehouse Growth: Climb Every Warehouse', 1st November, 2006, http://www.intelligententerprise.com/showArticle.jhtml?articleID=193105574

Wolpaw, J. R., Birbaumer, N., Heetderks, W. J., McFarland, D. J., Pfurtscheller, G., Vaughan, T. M. (2002), 'Brain-Computer Interfaces for communication and control', *Clin. Neurophysiol., 113*, pp. 767-91.

Wolpaw, J. R., McFarland, D. J., Neat, G. W., Forneris, C. A. (1991), 'An EEG-based Brain-Computer Interface for cursor control', *Electroencephalography and Clinical Neurophysiology, 78(3)*, pp. 252–59.

Teepe, W. (2006), 'Reconciling Information Exchange and Confidentiality. A Formal Approach', PhD thesis Groningen, available at http://www.teepe.com/phdthesis

WWRF (2001), 'The book of vision 2001', Version 1.0, Wireless World Research Forum, http://www.wireless-world-research.org/general_info/Bookofvisions/BoV1.0/BoV/BoV2001v1.1B.pdf.

Yeo, C. S., Buyya, R. (2005), 'Service level agreement based allocation of cluster resources: handling penalty to enhance utility', *In Proc. the 7th International Conference on Cluster Computing*, 2005.

Zeng, F.G. (2004), 'Trends in cochlear implants', *Trends Amplif., 8(1)*, pp. 1-34.