FIDIS

Future of Identity in the Information Society

Title:	"Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence"
Author:	WP7
Editors:	Wim Schreurs, Mireille Hildebrandt (VUB, Belgium) Mark Gasson, Kevin Warwick (Reading University, UK)
Reviewers:	Denis Royer (University of Frankfurt, Germany) Ioannis Maghiros (JRC, Spain)
Identifier:	D7.3
Type:	[Deliverable]
Version:	1.0
Date:	Friday, 05 August 2005
Status:	[Final]
Class:	[Public]
File:	fidis-wp7-del7.3.ami_profiling.doc

Summary

This document considers some of the wider aspects of privacy and security in the AmI environment as these are affected by profiling techniques and methods. It has been shown that by the very nature of the AmI space such issues are prevalent. Although it is unclear exactly how the AmI environment will develop, and indeed how it will be accepted by society as a whole, it is predicted that in some form AmI will appear in our everyday lives. However, AmI space requires a high level of profiling to be successful. Solutions for issues of privacy and security are usually located at a technological and a legal level, both implicating the social and the cultural. In this deliverable a first exploration of technological solutions and a first extensive exploration of relevant EU law is presented.

As to the technological level, the report discusses two privacy-enhancing techniques to provide pseudonymous customised services. In these models, the user is in control of his own data, and has an Identity Management Device (IMD) that manages his data, profiles and preferences. The IMD presents the user preferences to ambient intelligence devices in order to obtain personalised services. The first technique is based on anonymous credentials, and it may not be appropriate to be implemented in many ambient intelligence environments, as it requires costly resources. The second technique is adapted from the field of targeted advertising. It is cheap to implement, and ambient intelligence devices with low storage capacity and computation power could easily implement it.

As to the legal level, an extensive survey is made of the EU Data Protection Directive and other relevant sources of EU law, such as the Privacy and Electronic Data Communications Directive, and E-Commerce Legislation, Consumer Protection Legislation. This survey, focused on relevant implications for both group profiling and personalised profiling, and implications at the level of the collection of data, the construction of profiles and at the level of their application, should serve as a first inventory on which subsequent deliverables can build.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

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	25.03.2005	First draft Wim Schreurs (VUB)
0.2	25.03.2005	Edit Mireille Hildebrandt (VUB)
0.3	28.03.2005	Edit Wim Schreurs / Mireille Hildebrandt (VUB)
0.4	08.04.2005	Initial release Contributions of Sabine Delaitre (IPTS) and Claudia Diaz (COSIC)
0.5	31.05.2005	Contribution of Mark Gasson, Kevin Warwick (Reading) Edit and formatting by Mark Gasson (Reading)
0.6	02.06.2005	Contribution of Ronald Leenes (TILT)
0.7	22.06.2005	Contribution of Wim Schreurs (VUB)
0.8	01.07.2005	Final Edit (substantial restructuring) Mireille Hildebrandt (VUB)
0.9	05.07.2005	Final Edit Mark Gasson (Reading)
0.9a	01.08.2005	Comments internal reviewers
1.0	04.08.2005	Final version Mireille Hildebrandt, Mark Gasson, Wim Schreurs, Els Soenens

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)*
1	Mark Gasson, Mireille Hildebrandt
2	Wim Schreurs (2.1, 2.3, 2.4), Sabine Delaitre (2.2), Mireille Hildebrandt (2.5)
3	Wim Schreurs, Mireille Hildebrandt
4	Mark Gasson, Sabine Delaitre, Kevin Warwick
5	Wim Schreurs, Mireille Hildebrandt (5.1, 5.2), Ronald Leenes (5.3)
6	Mireille Hildebrandt, Wim Schreurs (6.1, 6.3), Claudia Diaz (6.2)
7	Wim Schreurs, Mireille Hildebrandt
8	Mireille Hildebrandt
9, 10	Els Soenens, Mireille Hildebrandt, All

Table of Contents

1 Executive Summary

According to many authors the aim of the Ambient Intelligence (AmI) environment is to provide a context aware system, using unobtrusive computing devices, which - in their vision - will improve the quality of people's lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf. Additionally, pervasive computing should enable immediate access to information and services anywhere, anytime.

To be able to offer such personalised operation, the 'intelligent' environment needs to build a profile of each individual, and be able to subsequently link the profile with the correct individual. In essence, the environment must become the interface to the distributed and invisible AmI. Thus profiling is an essential part of the idealised AmI. In a world where computing is truly ubiquitous, profiles will seamlessly follow the individual to whom it is linked.

This report provides a first analysis of actual and possible profiling techniques in the field of AmI and aims to describe some implications of such profiling techniques within AmI for privacy and security.

In Chapter 2 an initial description of AmI is provided, starting from a simple example concerning a 'Smart Home', presenting some of the definitions from the available literature, inferring the key notions of AmI: ubiquitous computing and communication; intelligence or adaptive systems; and personalisation or user empowerment. At the end of this chapter some of the fields of application are indicated as envisioned by the Information Society Technology Advisory Group. Chapter 3 focuses on the process of profiling in relation to AmI, referring to FIDIS deliverable 7.2 (*descriptive analysis of profiling*), to discriminate between group and personalised profiling and to discuss the difference between automated and predefined profiles. Chapter 4 gives a first overview of the technological aspects of profiling in an AmI environment. Chapter 5 indicates some of the privacy and security issues raised by the proliferation of personal data and real time - often personalised - profiles that seems inevitable in the current visions of AmI. Chapter 6 contains a first attempt to develop solutions to privacy and security issues via technologically facilitated end user control. In a sense such technological designs are pertinent if data protection legislation is to have any effect. Chapter 7 gives a first elaboration of the relevance of EU legislation concerning profiling, demonstrating that data protection legislation was written for the protection of personal data without much awareness of the intricacies of group profiling based on anonymised personal data, applied to non-identifiable persons.

This deliverable should be understood as a first venture into a domain that is yet to come into existence, argued on the basis of visions that depend on prototypes as yet not in full operation. We are dealing with a vision that is nourished by technological optimism while it nourishes technological dystopia. The full extent of the social and cultural implications that will determine whether and how something like AmI will come into existence should be dealt with in subsequent deliverables, starting with FIDIS deliverable 7.7 on RFID, AmI and profiling.

2 Description of Ambient intelligence (Aml)

2.1 Prologue

To date, many research projects have been launched in the area of Ambient Intelligence (AmI). The researchers in this field often refer to the same sources and references, of which the reports of the Information Society Technology Advisory Group (ISTAG) are the most prominent. We will build on this literature and provide a first listing of relevant sources in the bibliography. In this section we aim to introduce the concept and some of the unfolding realities of AmI. We start with a simple example of a smart home, to introduce some of the basis features of an intelligent environment,[1] after which we will look into some of the definitions provided by ISTAG and others. They will highlight salient aspects of the AmI vision, for example the fact that it is based on interactive networked environments that function like an intelligent interface between users and their contexts. In the next paragraph AmI will be described in terms of three key concepts: ambience (ubiquitous computing and communication), intelligence (or adaptiveness) and personalisation (empowerment of the user). This chapter will end with a listing of possible fields of application, as foreseen by the ISTAG.

2.2 Ambient intelligence Space example: The Smart Home

2.2.1 Introduction

Ambient Intelligence (AmI) aims at enriching the quality of the everyday experience and places human beings at the centre of the future development of the knowledge-based society and Information and Communication Technologies. Thus, the AmI vision is based on a user-driven approach and encompasses three main technologies: ubiquitous computing, ubiquitous communication and intelligent user interface, with a view to delivering seamless applications and services to citizens. The user's context is an indispensable component of this approach taking into account the needs of the user by responding in an appropriate way (personalisation).

Profiling activity consists of extracting useful information from a current context related to the user, identifying the users' needs and selecting suitable services in order to enable that the smart home behaves according to the users' preferences, actions and expectations. Consequently, profiling activity is essential to achieve an aware, adaptive and responsive environment, in turn, to meet the user needs and wishes.

In the next section, we will first introduce and describe the Smart Home regarded as a private AmI environment. We will also study the profiling activity in AmI space and will introduce topics such as feasibility examined from a specific point of view dealing with social, technical and legal aspects. Additionally, we shall consider user control, or more precisely the conflict between profiling activity and user control and the necessity to use Intelligent Agents to regulate such conflict. Because profiling involves the communication and exchange of a user's

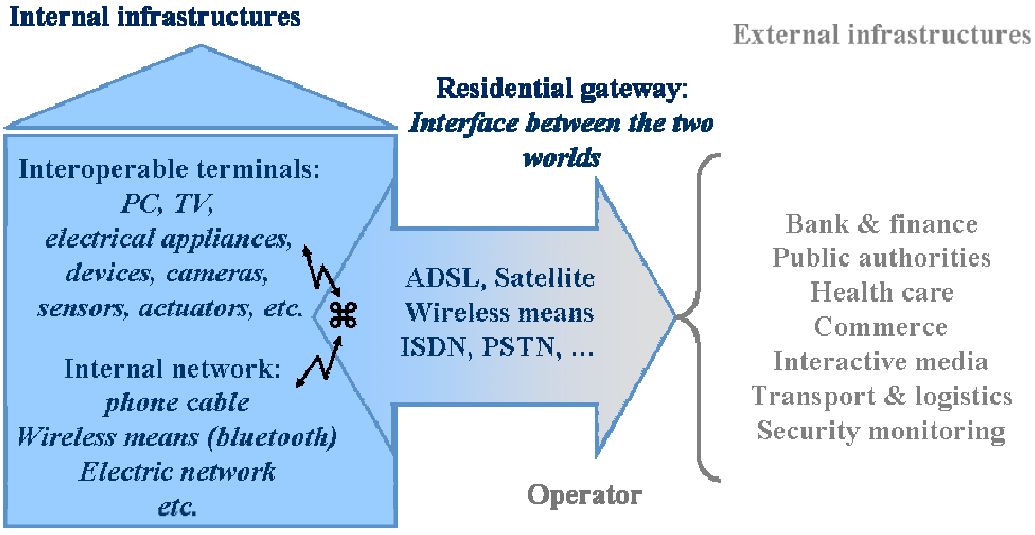
[1] See also the examples of AmI scenario's at http://www.ist-eperspace.org/. This is the website of one of the IST projects (ePerSpace) regarding AmI within the Sixth Framework Programme (Project no: IST-506775). See the bibliography under the heading of 'Relevant Internet Portal' for other projects and relevant sites.

personal data and their storage, we will also indicate some of the security and privacy concerns involved.

2.2.2 The Smart Home: Elements and Services

AmI in the home environment, known as the 'Smart Home', aims to integrate the systems and technologies developed to run the household for improved management of the home environment. The Smart Home is equipped with surrounding technologies used to turn devices and appliances on and off or to send and receive information.

Figure 1 describes the different elements of the Smart Home.[2] The internal infrastructures are essentially composed of interoperable terminals and the internal network. The residential gateway plays an important role as the interface between internal and external infrastructures and to services of operators.



ISDN: Integrated Services Digital Network

PSTN: Public Switched Telephone Network

Figure 1: Elements of the Smart Home infrastructure

The smart home services can be categorised into four groups,[3] detailed in Figure 2:

- Communication Services
- Home Control and Automation

[2] Menduiña E., *Integration of biometrics in Smart Homes*, 2nd BioSec Workshop, Brussels, January 2005. And Clements, B., Maghiros, I., Beslay, L., Centeno, C., Punie Y. & Rodriguez, C. *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS-JRC, July 2003.

[3] Plomb, J. and Tealdi, P., *Ambient Intelligent Technologies for Wellbeing at Home*– EUSAI 2004, Eindhoven, The Netherlands.

- Entertainment
- Home Networking

The Smart Home has to behave automatically according to the user's preferences and expectations. In order to achieve this objective, profiling activity has to be implemented.

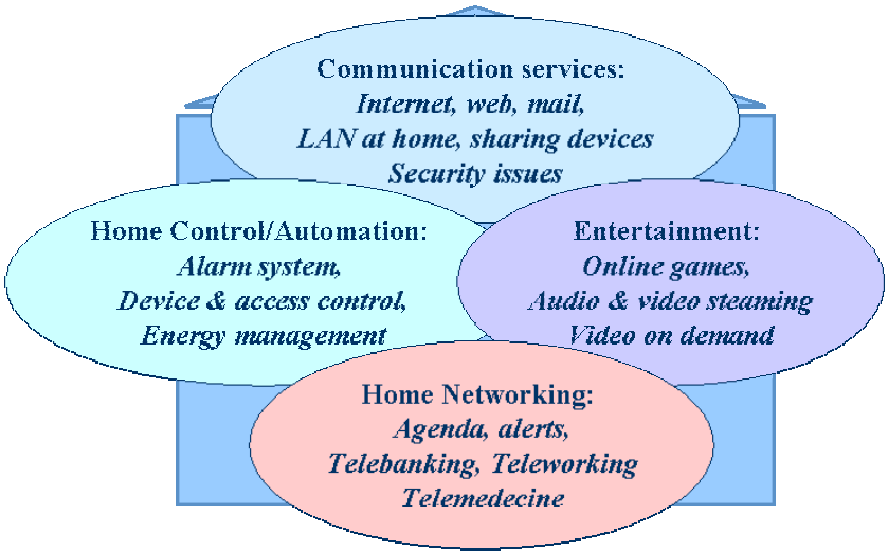


Figure 2: Smart Home Services[4]

2.2.3 Profiling activity

One of the main objectives of AmI is to meet the user's needs; profiling activity is thus required. Profiling activity for this purpose is a continuous background activity; it includes extracting useful information from a user and his/her current context (for example user location, user behaviour, room temperature), enabling the identification of the user's needs, selecting suitable services and adjusting the parameters of the selected services in order to allow the AmI environment to behave according to the users' preferences, actions and expectations. Consequently, profiling activity is essential to achieve an aware, adaptive and responsive environment, and thus, to meet user needs and preferences. Hence, if profiling does not work adequately, the vision of AmI may never be realised. Profiling activity is depicted in the schema below (see Figure 3).

Some elements (see the blue rounded rectangles) are concrete elements and are closely related to profiling activity. The other elements (pink rectangles) are spatial elements, particularly relevant to the AmI space. They make the collection of useful data for the profiling activity easier (environmental awareness aspect) and help to transmit/apply the results of profiling (responsive aspect) in a suitable way (adaptive aspect). The key technologies mentioned above play an important role in this activity: ubiquitous computing and communication

[4] Menduiña E. 2005.

support the tasks related to the two first aspects and intelligent user interfaces allow the achievement of the last one.

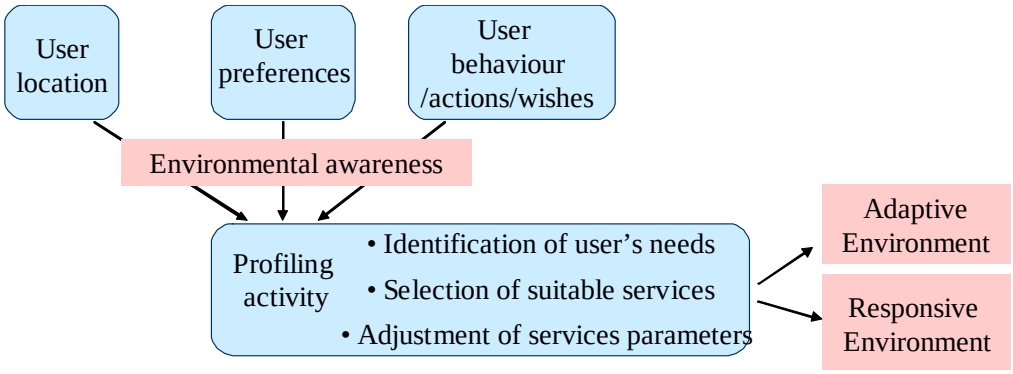


Figure 3: Schematic view of profiling activity in the AmI environment[5]

For the purpose of this example we understand a profile as a set of correlated data that identify and represent attributes, behaviour and rules of engagement, either of the end-user or of the service provider.

The *end-user profile* includes the user's "identity" (it may only be necessary to get an identifier or to use an identification mode), and his/her inferred needs and preferences.

The *service profile* describes the parameters of the service, the operational requirements and the availability of the service.

2.2.4 Multi-user environment

Difficulties may arise when the preferences and/or requirements of the several users that are present are contradictory or overlapping. The Smart Home is an example of a multi-user environment, and profiling activity has to resolve such conflicts. For example a conflict over the use of shared resources is quite common, i.e. sharing of facilities or services between different users such as one TV in a home. One solution is to merge profiles to concurrently respond to the users or to direct a specific environment/material/facility to the users depending on priorities established during the merging process.

2.2.5 Security and privacy concerns

Profiling activity thus involves the proliferation of communications, exchanges of personal user data, and identity information, and their storage by means of numerous types of technologies, sensors and devices. Therefore, security and privacy concerns arise when profiling activity is carried out. In the case of the Smart Home, the home network is regarded as the means used to communicate the profiling information. Ideally, profiling activity requires continuous monitoring or surveillance of the users. The use of sensors is crucial since they make it possible for example to detect that a person is entering a room or an object is

[5] Sabine Delaitre, Identity: facets and vulnerabilities in ambient intelligence environment, in *EICAR 2005 conference*. ISBN:87-987271-7-6, pp 154-166.

being moved, etc. In the case of a video camera, this sensor may be perceived as invasive, since it is possible to identify and store who entered or who moved the object.

If such monitoring is used in a particularly private space such as a bathroom, users may feel this activity is an unacceptable intrusion. In any case, such monitoring and surveillance may erode privacy and since large amounts of data may be stored, fears about personal data theft arises. As such, Privacy Enhancing Technologies (PETs) like Identity Management Systems (IMS, type 1, cf. FIDIS deliverable D3.1) should be developed to protect the users against this threat. It should be noted that this monitoring could be worthwhile for medical purposes, to ensure medication is taken, or to assess the current condition of the user. In any case, in the AmI vision profiling must respect the decisions and requirements of the users. Hence this space has to be equipped with mechanisms ensuring confidentiality and managing authorisation rights.

2.2.6 Feasibility

The Ambient Intelligence space requires a continuous profiling activity. This section draws up a list of requirements for this activity by taking into account three dimensions: social, legal and technological.

- From a social point of view, the Ambient Intelligence space and thus the profiling activity has to increase well-being, to ensure trust,[6] to respect privacy and to provide safety. As previously discussed, these points are the challenges of profiling and will be discussed further in Chapter 5.
- From a legal point of view, many aspects have to be considered such as Digital Right Management (DRM)[7] and Data Protection (DP). For instance a Mobile DRM[8] could be described as a set of actions, procedures, policies, product properties, and tools that an entity uses to manage its rights in digital contents according to requirements over mobile networks. The legal issues will be discussed extensively in Chapter 7.
- From a technological perspective, standards and security are the pillars of AmI that need to be established.[9] Further discussion of standards and technical infrastructure is given in Chapter 4.

[6] Dinka D. and Ingmarsson M. A*mbient intelligent at home,* White paper in the EU-founded project Ambient Intelligence To Go: AmIGo.
[7] See for instance the *Mobile Digital Rights Management White Paper* 2003, of the NEC corporation, available at: http://www.nec-mobilesolutions.com/application/products/drm.html.
[8] Zheng Yan, *Mobile Digital Rights Management,* T-110.501 Seminar on Network Security 2001, Publications in Telecommunications Software and Multimedia TML-C7, Espoo, 2002.
[9] Robbie Schaefer, Heinz-Josef Eikerling, Increasing the Acceptance of Ambient Intelligent Technologies for Wellbeing at Home through Security Contexts – *EUSAI 2004*, Eindhoven, The Netherlands.

2.2.7 Conflict with user control

Direct User interaction is a common way by which a user is able to control appliances, monitor their state and program various intelligence embedded appliances to for example aid with automatic data acquisition. A possible conflict may occur between profiling activity and user control. The question "what is good, beneficial profiling?" may arise (see Figure 4).

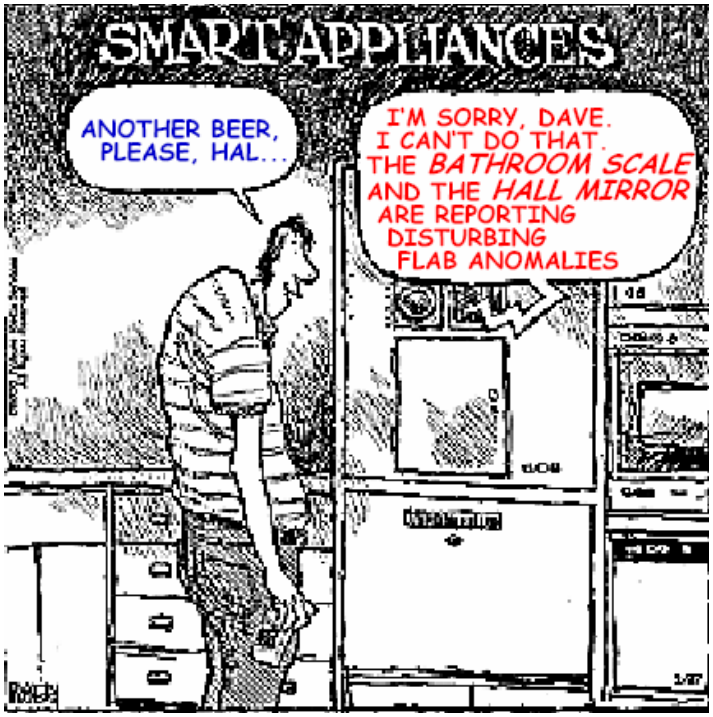


Figure 4: 'Smart Appliances': A conflict between user control and profiling activity (Illustration by J. MacNelly)

Indeed, sometimes profiling activity ('*service to user'* or '*environment push'*) comes into conflict with user control ('*user to service'* or '*user pull'*). The objective is to find the right balance in order to minimise this type of conflict.

2.2.8 Profiling for online life

Generally, in a complex domain space, such as the online part of the AmI environment, it is difficult for the user to express his needs or in some cases even to know what he wants. As such, the expression of requirements is minimal or incomplete. Using an Intelligent Agent may solve part of this problem.[10] Essentially the software of the Intelligent Agent embodies the profiling activity and supports users in decision taking, learning about the domain, creating a profile or exploring sample sets.

[10] G. M. P. O'Hare, M. J. O'Grady, S. Keegan, D. O'Kane, R. Tynan & D. Marsh, *"Intelligent Agile Agents: Active Enablers for Ambient Intelligence,"* AISD, SIGCHI workshop, Vienna, 2004.

Intelligent Agents allow personalisation and discovery to take place at the level of the user, as the agent infers a user's preferences from the interactions with the environment. These then do not have to rely only on data entry as a form of user interaction.

2.3 AmI: science fiction or unfolding reality?

In this section the various descriptions of AmI are discussed. The concept refers to something that is more than just science fiction, but it is still unclear to what extent it represents an unfolding reality. Descriptions in the relevant literature underline this point:

- **ISTAG**: *Scenarios for ambient intelligence in 2010* describes AmI as a vision where '(…) people will be surrounded by intelligent and intuitive interfaces embedded in everyday objects around us and an environment recognising and responding to the presence of individuals in an invisible way. (…) It puts the emphasis on user- friendliness, user-empowerment and support for human interactions. AmI stems from a convergence of three key technologies: Ubiquitous Computing, Ubiquitous Communication, and intelligent user- friendly interfaces. It implies a seamless environment of computing, advanced networking technology and specific interfaces. (…) This intelligent environment is aware of the specific characteristics of human presence and personalities, takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire, and even can engage in intelligent dialogue'.[11]

- **RIVA et al.**: *Being There: Concepts, effects and measurement of user presence in synthetic environments*, state that 'Ambient Intelligence (AmI) refers to a new paradigm in information technology, in which people are empowered through a digital environment that is aware of their presence and context, and is sensitive, adaptive, and responsive to their needs, habits, gestures and emotions (…) All the environment around us, homes and offices, cars and cities, will collectively develop a pervasive network of intelligent devices that will cooperatively gather, process and transport information (…) AmI is the direct extension of today's concept of ubiquitous computing, i.e. the integration of microprocessors into everyday objects. However, AmI will also be much more than this, as the AmI system should adapt to the user's needs and behaviour." [12]

- **Van Loenen**, Philips' project manager of the **Ambience** Project (finished in 2003)[13], says Ami "builds on advanced networking technologies, which allow robust, ad-hoc networks to be formed by a broad range of mobile devices and other objects (…) By adding adaptive user-system interaction methods, based on new insights in the way people like to interact with computing devices (social user interfaces), digital environments can be created which improve the quality of life of people by acting on their behalf."[14]

---

[11] ISTAG, (Information Society Technology Advisory Group), "Scenarios for ambient intelligence in 2010", 2001, p. 1.

[12] Riva, G., Loreti, P., Lunghi, M., Vatalaro, F. & Davide, F., "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, 2003, 344 p. Quote taken from the on-line version, available at http://www.vepsy.com/communication/book4/4_04RIVA.PDF, p. 5.

[13] See http://www.itea-office.org/projects/facts_sheets/ambience_fact_sheet.htm

[14] Van Loenen, E., "On the role of Graspable Objects in the Ambient Intelligence Paradigm", proceedings of the Smart Objects Conference, May 15-17, Grenoble, France, available at http://www.grenoble-soc.com/proceedings03/Pdf/Van%20Loenen.pdf p. 1.

- **Bohn et al.**: *Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing*: 'Visions of ambient intelligence and ubiquitous computing involve integrating tiny microelectronic processors and sensors into everyday objects in order to make them 'smart'. Smart things can explore their environment, communicate with other smart things, and interact with humans, therefore helping users to cope with their tasks in new, intuitive ways'. [15]

Obviously, the phenomenon of AmI does not yet exist *as such* in today's life. It is impossible to predict *if* and in particular *how* this evolution towards AmI will take place. But we can see many emerging technologies, supported by standardisation, social acceptance and legal frameworks, which could facilitate AmI. We refer amongst others to wireless online environments, internet access on the basis of flat fee subscriptions, electronic identity cards, biometrics, electronic commerce, LBS (location based services), GPS (global positioning systems), RFID (radio frequency identity tags), increasing storage capacity and processor speed, research in the field of nanotechnology and in the area of brain-computer interfacing.

The decrease of the cost of these technologies as well as the emergence of customers that are willing to pay for the services that can be provided seems to increase the likelihood that at least some kind of AmI practices will surface. Besides these supporting technologies, techniques of user modelling and profiling are already widely spread, providing customers with enhanced, personalised and customised services (e.g. Amazon, customisation in financial offers). There seems to be a smooth connection between targeted advertising, customised servicing and ambient intelligence.

2.4 Key concepts of AmI

Several concepts concerning AmI seem to be highly relevant, distinguishing AmI from other types of personalised services. Here we will pay attention to the **ambient** aspect, which includes both **ubiquitous computing** and **ubiquitous communication**, and the **intelligence** that is based on ubiquitous communication by means of **intelligent interfaces**. Lastly we will focus on the central concept behind AmI, which is **personalisation** of the environment, indicating the 'human centred' focus of AmI- applications.

2.4.1 Ambience: Ubiquitous computing and ubiquitous communication

One of most striking features of AmI is the fact that it will be embedded in everyday objects around us in an invisible way. This indicates both pervasive and ubiquitous computing and communication. It is in fact the disappearing interface that characterises the ambient aspect, or, in other words, the environment (the multiplicity of smart things we run into) becomes the interface. The software is hidden and works automatically to such an extent that people are less aware of it or even not aware at all. The idea is that we get used to AmI without constantly realising the presence of intelligent devices. This aspect is not new, we are already surrounded by systems and products with embedded computers like in televisions, intelligent TiVo recorders, cars and other means of transportation, machines, energy and communication systems. What is new is the real time wireless communication between technologies

[15] Bohn, J., Coroama, V., Langheinrich, M., Mattern, F. and Rohs, M. 2004, "Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing", Institute for Pervasive Computing, ETH Zurich, Switzerland, p. 1, available at: www.vs.inf.ethz.ch/publ/papers/socialambient.pdf.

embedded in the environment and technologies carried by the human person, and linkage to data records held on the internet, a remote database or a personal digital assistant. This ubiquitous communication allows the customisation of an environment, by means of the software *intelligence* that will be introduced (through micro-processors) into many objects like television and cars, but also shoes, clothes, money, food, washing machines, walls, doors, heaters, windows, etc.

2.4.2 Intelligence

Other than 'conventional' forms of ubiquitous and pervasive computing, AmI constitutes an 'intelligent environment' that is aware of the specific characteristics of a human person in a specific context. By means of intelligent devices the environment adapts or *learns* about the *needs* of a specific human person, based on her past behaviour. On top of that, the intelligent devices allow the environment to *respond intelligently* by reorganising the environment according to the preferences of the human person, deducted from patterns in past behaviour. In other words, the intelligence consists of:

a. Collecting, recording and processing data concerning a specific human person and her environment;
b. Inferring her preferences;
c. Responding by readjusting the environment according to these preferences; and
d. Storing the preferences by readjusting stored profiles in real time to continue the process of providing up to date intelligent responses.

2.4.2.1 Example of intelligent showers

The definition of the term intelligence can, at this stage, best be explained by a simple example:

A household of four people uses a thermostatic shower that can (but *must* not) be activated with a fingerprint. Each fingerprint is linked to an individual. When a certain member of the family takes a shower for the first time, the default temperature is 26 degrees. After several showers, the software will deduce from the behaviour of an individual that he likes a temperature of about 18 degrees. For instance after taking three showers, the default temperature for that individual will become 18 degrees instead of 26 degrees.

By automatically collecting the shower activity of an individual, the shower 'learns' that the individual likes relatively cold showers of 18 degrees. If, due to a cold winter, the individual adjusts the temperature to 24 degrees, the default position will be automatically changed to 24 degrees. The same applies to the other members of the family. Now, when this person takes a shower in a hotel that uses the same technology, the shower in the hotel could also adjust the shower temperature to the preferences of the individual - if the *profile* of this individual is communicated to the Hotel shower software.

In this deliverable, one of the pertinent issues is whether it is possible to store the dynamic profile on the personal device of a user, instead of a network or a remote database, and - if possible - to which extent this falls within the scope of Ambient Intelligence. In a further elaboration of the example, the profile could take into account more specific situations, such as a person taking a shower after a tennis game prefers much colder water than when taking a shower in the evening, etc.

As to the use of the term intelligence, it should be stressed that this intelligence depends on the one hand on the input of those that write the software and the algorithms involved i.e. computers only act according to the codes written for them. However, on the other hand, the intelligence of the software depends on the fact that the software moves beyond the original input, building on emerging patterns and thus learning in the sense that knowledge is constructed, applied, reconstructed and so on. Whether this type of learning measures up in any significant way to human learning and human intelligence is out of this document's scope, however, the fact is that the computing powers of the hardware involved are far beyond those of humans. This allows computers to produce correlations based on enormous sets of data not usually accessible to a human mind. The speed with which these correlations can be made and the fact that they are made on the basis of algorithms designed by a human person, brings to mind a tortoise slowly following its path: 'I may be going slowly, but then I may be going in the wrong direction'. However fast a computer works and however complex the correlations found, a computer can do nothing other than apply a code written by a human person.

The interesting question is perhaps not whether computers can think or whether they are intelligent, but in which way they think differently (or their intelligence works differently) and what this should mean for the application of computer technologies.

2.4.3 Personalisation

In principle, AmI technologies could be used to create a responsive environment for animals or even plants, allowing a reduction in the cost of human intervention, for example, in cattle-breeding (AmI in the stable) or horticulture (AmI in the greenhouse). One could, for instance, imagine a Smart Home that provides personalised services for a cat that is left alone for some days (regulating temperature, providing the right amount of food in time, maybe some robotic device to clean the litter tray). In this case we are not talking about personalisation, as the environment will only have to deal with a set of plants or animals, not persons.

In this deliverable we will focus on AmI as a technology to personalise the environment of individual human persons. This personalisation can consist of providing all kinds of services without an explicit action on the part of the 'customer', but it can also consist of taking over routine decision-making processes, thus reducing the amount of choices to be made without loosing out on interesting opportunities. The point here is that the intelligent device continuously constructs and reconstructs behavioural profiles that indicate certain preferences, enabling the construction of a responsive environment that seems to know one's preferences before they have surfaced in consciousness.

The human-centred approach and the concept of personalised services is important because it indicates that the AmI system needs a never-ending stream of personal data to (re) construct personal profiles that indicate what people want and to provide them with customised services. Thus in order to *provide* personalised goods and services, AmI needs to *be provided with* personal information. The more (useful) personal information the AmI system has access to, the more personalised (and intelligent or enhanced) its services can be. It should be noted that precisely this aspect of AmI raises questions about privacy and security.

2.5 Possible applications of AmI

In the ISTAG report of 2003, *Ambient Intelligence: from vision to reality*, empowerment of ordinary people by means of AmI is emphasised over and against a systems view of AmI. According to the report the focus should be on facilitation of end users, enhancing their opportunities to participate. Insisting that AmI should be treated as an imagined concept or an emergent property - not as a set of specified requirements, the ISTAG pleads a holistic approach to AmI. Instead of defining the concept it strives to create a vision of AmI that is still in the making, dependent on stake holder's consensus (promoting open standards), end user trust (control) and a plurality of scientific perspective (computer science, cultural studies).

The following eight fields of application are presented as exemplary for the emancipating potential of this holistic AmI vision:

1. Community building: reinforcing existing bonds and formation of new social groups;
2. Health care: e.g. creating smart homes with responsive and pro-active health care environments;
3. Smart home: building a comfortable cocoon and facilitating flexible participation in work and other relations;
4. Civil security: AmI should allow a move form traditional monitoring tools to advanced forms of risk assessment and decision support;
5. Environment: the same move from traditional monitoring tools to real time profiling technologies could greatly enhance both the diagnosis and the sustainability of environmental developments;
6. Mobility and transport: virtual mobile environments (SMEs) can be constructed;
7. Sustainability: AmI could facilitate new technologies;
8. Enterprise: enabling the formation of virtual enterprises.

The utopia that seems to await us in the near future as we build the infrastructure to facilitate the vision of AmI to become reality must be regarded with some sober scepticism.[16] As the ISTAG and reports of many others stress, technology in itself will not solve all our social problems. What is important, however, is to keep track of the process of emerging AmI technology design, anticipating the implications of different types of design.[17] In this FIDIS Workpackage the focus is on the aspect of profiling technologies, on which the vision of AmI (and its reality) seems to depend. We shall thus briefly refer to the finding of FIDIS deliverable 7.2 "Description and analysis of profiling practices" followed by special attention to the relevant issues for profiling in the AmI environment.

[16] Aarts, Emile and Stefano Marzano. 2003. "The New Everyday. Views on Ambient Intelligence", Rotterdam: 010., see p. 22-53 for a critical assessment. An interesting analysis of the social, economic and ethical implication is made in Bohn, J., Coroama, V., Langheinrich, M., Mattern, F. and Rohs, M. 2004, 'Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing', Institute for Pervasive Computing, ETH Zurich available at: www.vs.inf.ethz.ch/publ/papers/socialambient.pdf

[17] About 'upstream' participation in technological design, see Irwin, Alan. 2001. "Citizen engagement in science and technology policy: a commentary on recent UK experience", *PLA Notes* 40.

3 Description of Profiling in relation to AmI

3.1 Personalised and group profiling

In FIDIS Deliverable 7.2, profiling is defined as:

"The process of constructing profiles (correlated data) that identify and represent a person or a group/category/cluster, and/or the application of profiles to a person as a member of a specific group/category/cluster".

As has been mentioned in FIDIS deliverable 7.2, the concept of personalised profiling is of great importance for AmI, as AmI is basically the most radical and extensive form of targeted servicing one can image. Personalised profiling aims to construct profiles that allow targeted advertising, targeted servicing and customisation; AmI revolutionises such applications. We shall briefly refer to the distinction made in deliverable 7.2 between personalised and group profiling.

- Group profiling concerns the construction and/or application of correlated data sets, based on searching large databases. The correlations and patterns that emerge can highlight specific characteristics of an already existing group (like the members of a political party, members of a class in high school) or they can form the construction of the group/cluster/category itself. Group profiling is relevant for AmI in as far as service providers use group profiles to service their customers.
- Personalised profiling concerns the construction of a set of correlated data, on the basis of data processing of one particular individual. For AmI, personalised profiling seems the most exemplary, because AmI aims at providing seamlessly customised (individualised) services.

3.2 Profiling in AmI design

3.2.1 Profiles: predefined, automated and other types of profiles

In the beginning stages of AmI it may be the case that end-users and AmI service providers work with predefined profiles. The service provider may target certain customers (for instance of a certain age) and the end-user may provide input via a deliberately constructed profile (set of preferences concerning a specific environment, for instance a restaurant, hotel, car). In that case AmI does not make use of profiling technologies in the sense of this Workpackage, and one can doubt seriously whether we can - in that case - speak of an intelligent environment, since the environment does not 'learn' (only applies predefined profiles).

We shall distinguish this type of profile as 'sets of data' from the type that is derived from profiling technologies (the focus of this Workpackage) as 'sets of correlated data'.

In FIDIS deliverable 7.2 user modelling and user adaptive applications are discussed as a type of personalised profiling. To some extent this type of profiling does not depend only on data mining techniques, as it makes use of direct input by the end-user, simple extraction out of data bases (without use of stochastic data mining techniques), capture of user's activities and

inference from other type of information. User modelling seems a mix of predefined profiles, automated profiles and human intervention, thus being more elaborate and more sophisticated than data mining itself. It seems however that user modelling does result in a dynamic set of correlated data, which is used as a knowledge construct to create an adaptive environment, so the profiles that are generated during a process of user modelling do fall within the scope of profiles as sets of correlated data.

3.2.2 The context of the human person

An AmI environment should - in order to function as proposed - not only profile the data subject whose environment will be customised, but also this subject's context. To make the environment adaptive to the inferred preferences of the subject, the context itself will have to be profiled. This concerns data like room temperature, volume of the audio-set, amount of light and/or the presence of certain objects and even, to complicate matters, other subjects that have an equal 'right' to personalised services in the particular environment. This would mean that, as far as nonhumans are concerned, the definition of profiling should be rearticulated as:

"*The process of constructing profiles (correlated data) that identify either a data-subject or a group/category/cluster, and/or the application of profiles (correlated data) to a data-subject as a member of a specific group/category/cluster*."

As indicated in the glossary, a data subject is the subject (human or nonhuman) that the data refer to/describe/are attributed to. By using the term data subject the scope of profiling is widened to include any human, animal or thing of which data are processed and stored.

4 Technological aspects of profiling for AmI

4.1 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. As already discussed, 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 7.2 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 4.1.

4.2 The essence of AmI

AmI itself will not be the outcome of any single technology or application; rather it is an 'emergent' property.[18] Essentially, AmI is more than just the sum of its parts. Ubiquitous Computing, a key aspect of AmI, 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. 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 is 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 subsequently to 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 monitor direct interaction of people with objects and profiles will seamlessly follow the individual to whom it is linked.

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

4.3 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:[19]

- **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.

The scale of this issue is highlighted by examining the levels of interaction that may occur between the user and the technology within this AmI context. The 'MultiSphere Reference Model'[20] is shown in Figure 5.

[19] ISTAG, "Scenarios for ambient intelligence in 2010", 2001.

Figure 5: The MultiSphere Reference Model[20] showing various layers of interaction desirable in the AmI scenario

Although this model is aimed primarily at putting issues and ideas of wireless communication in context, from it, and similar models, the following interaction levels have been identified:[21]

- 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 fulfill 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

[20] 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.
[21] Riva, G., Loreti, P., Lunghi, M., Vatalaro, F. & Davide, F., "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, 2003, 344 p.

protocols. Only in this way will adequate profiling activity be realised, utilising the mass of data which such systems make accessible.

4.4 Technical aspects of Profiling in AmI

To fulfil the full AmI vision, it is proposed that the AmI acts according to the user's preferences, needs and expectations, thus profiling is the key stone of this scenario. From an implementation perspective, the 'intelligent agent' is the embodiment of the profiling aspect which attempts to build a comprehensive profile of the user by processing data recorded from his or her interactions, behaviour, preferences, and essentially 'learning' by interpretation of these events in their context. FIDIS deliverable 7.2 has previously examined the data mining techniques which could be adopted for the data processing phase.

From a purely pragmatic viewpoint, the agent needs to interact with or 'read' from the environment (for example from the thermostatic value in the example given in section 2.4.2.1) to retrieve data and with services to provide the user with the desired level of support. In some cases, such as 'online profiling' it is possible to easily compile personal data from Internet Protocol traffic (e.g. domain names visited, internet services used, etc.), from website log files (e.g. time, history of visited pages or images downloaded), from internet cookies (useful information in order to recognise the visitor, e.g. registration information, number of customer, tracking of activities, etc.) or simply from user data input to websites. The relative ease of this data collection is a result of the standardised methodologies that are employed for interacting online. However, data collection within the AmI environment becomes significantly more complex because it is the complex interaction with a large variety of objects and services within a specific context that requires analysis. In the most part, these objects and services currently are not networked in any way at all.

As such, within the AmI environment, it is clear that a seamless interoperable data flow between the various interaction levels shown in Figure 5, by proprietary devices from varying manufacturers, needs to be realised. This is only possible if the integrating network technology used is able to support systems integration, i.e. through standardised protocols. Some standards already exist such as CC/PP (Composite Capabilities / Preferences Profile) from the World Wide Web Consortium (W3C)[22] and UAProf (User Agent Profile) proposed by the Wireless Access Protocol (WAP) forum[23]. Notably, CC/PP is a standard based on Resource Description Framework (RDF), and is already used. Additionally, a number of standards for open communication in sensor networks have been proposed. Efforts to make buildings smarter are focusing on cutting costs by streamlining building operations, such as lighting and air conditioning. The most common networks are the BACnet and LonWorks standards, developed for building automation. These standards are geared towards well-defined application areas, and are built on top of well defined network structures. The net result of being so application specific is that many of the visions for AmI cannot be readily implemented on such systems. In practice, from the technical viewpoint, this may indicate that the AmI scenario is already running into issues of interoperability. A discussion of the sensor technologies that may be employed within the AmI network structure will be given in future FIDIS deliverables, starting with FIDIS deliverable 7.7 on RFID, AmI and profiling.

[22] http://www.w3.org/
[23] http://www.wapforum.org/

From a technical perspective, the process of forming a profile - even given access to the information required from the environment - is a computationally expensive process. Although developments in computing power are clear, it is supposed that the data mining of this vast amount of information will actually be implemented in distributed computing structures. As such, a standardised and interoperable agent that is abstracted from the underlying hardware such that it operates irrespective of the medium it is running on is required.

It is reasonable to note here that ultimately the price for such increased data flow is likely to be borne by a decrease in potential user privacy as personal information becomes readily and widely linkable. In chapter 5 some of the questions regarding privacy and security of this data are surveyed, while in chapter 6 some proposals are made to store the resulting profiles on the user's own personal digital assistant.

5 Impact of Profiling and AmI

5.1 Risks and opportunities

As it was concluded in FIDIS deliverable 7.2, profiling raises questions of trust, usability, security and privacy. AmI is focused on providing an environment that infers preferences on the basis of past behaviour, and provides services that create comfortable homes, takes away routine choices, signals useful opportunities and thus creates both extra time and a better picture of the risks and options we face.

All that was indicated in the "*Purposes and effects of profiling practices*" chapter of FIDIS deliverable 7.2 can be repeated here to describe the impact of AmI, in particular the risks and opportunities connected with customisation and de-identification. Will our lives become boring in the process of total customisation? Will our capacity to react adequately to new information diminish? Will our dependence on this 'magic' space prove fatal once this space ceases even momentarily to exist? Will Ambient Intelligence create serious risks for public health, by allowing people to get what they want without making a move (what is the benefit of a coffee machine that knows what coffee I want, other than the fact that I do not have to raise my arm, is that a benefit)? Will those that have the money to live in AmI environments be advantaged compared to those that do not? Will this increase existing inequalities or change existing hierarchies? We also refer to the evaluation of the "*Implications of profiling for democracy and rule of law*" in FIDIS deliverable 7.4.

In this report we will focus on some of the implications for privacy and security, leaving the discussion of other risks to subsequent deliverables.

5.2 Privacy aspects

Profiling technologies need a seamless, unobtrusive 'flow' of personal data. In this report several options are considered to store and/or process these data with the end user (chapter 6) instead of storing them in distributed networked systems or central databases, as this may violate privacy (rights) or create the risk of abuse.

Proliferation of personal data facilitates the construction of group profiles, as described in section 3.1 and of different personalised profiles of the same physical person, depending on the role this person plays in a specific context. Access to either the data and/or the dynamic profiles of a specific individual could lead to the construction of a complex and comprehensive profile that may seem to describe the 'reality' of the profiled individual. In combination with advanced personalised services, this comprehensive, real time, dynamic, profile would basically infer future behaviour from past behaviour. Could it be that targeted services and adaptive environments lead to a person living - in a sense - in a sophisticated and comfortable cage? If group profiles are integrated with personalised profiles the tendency to normalise those that did not fit the group profile in the first place into behaviour that fits the profiles.[24] The point is that the end user that is the target of all this enhanced servicing seems to be made transparent to an extent that was previously unthinkable. This transparency of the end user to the data user (the service provider, or some government agency that is interested in profiling the individual to prevent crime, illegal immigration, health risks, terrorism, or tax

[24] For instance in case of a non-distributive group profile, see FIDIS deliverable 7.2 on this issue.

evasion) contrasts starkly to the invisibility of the process of profiling and its end results. Even if data protection legislation would be effective, such that end users have access to their data and are empowered to correct or delete them, the sheer amount of data and profiles seems to make any significant access an illusion.

The problem in terms of privacy is the grip data controllers may have on the unconscious behavioural patterns that steer an individual as these could be used to modify or manipulate her future behaviour.[25] So, while AmI is 'sold' as a technology that will empower citizens to participate in public and private life to a much higher degree, it may well provide - at the same time - the tools to steer this participation to a previously unknown extent. The challenge will be to envisage technological design and legal regulation that can prevent such personal transparency and/or bring it under the control of the end user.[26]

5.3 Security aspects

Not only do personalised and group profiles reveal a 'reality' of a profiled person, also the fact that these data can be associated to personally identifiable information (PII) pose a risk. One of the risks incurred by the potential access to PII, is that of identity theft and identity fraud. These crimes are clearly on the rise in recent years, partly due to the fact that more and more activities are handled online.[27] In cases of ID theft typically PII, such as social security numbers, credit card numbers, or Social Fiscal numbers, are taken from victims without their consent in order to commit other crimes (see FIDIS deliverable 5.2 for a detailed account on ID fraud/theft). Identities are usually taken to conceal one's original identity (in order to acquire a visum for instance), to make some financial profit from some form of fraud (obtaining a credit card under a false identity, for instance), or to avoid financial liability (e.g. tax avoidance). In the context of AmI profiles, AmI introduces two types of risks with respect to ID fraud/theft. Firstly, PII can be part of, or associated to the profile, for instance as stored on a personal Identity Management Device (IMD) and thus be a target for ID fraudsters. IMDs most likely will contain PII. If these data are not secured properly, perpetrators could gain access to these data and copy it for criminal purposes. As AmI devices are likely to communicate by means of radio signals (RF), perpetrators can either try to hack the IMD to gain access to the data, which may be a criminal offence, or they may try to intercept the transmission of PII from IMD to remote devices. To minimise these risks, the IMD should be equipped with security measures to limit the possibilities of hackers getting access to the data stored in the IMD. With respect to the data transmission, risks can be limited by minimising the transmission of PII altogether, and if PII should be revealed data transmission should be properly protected by encryption techniques.

A second type of risk associated with PII is that the profiles, or part thereof, can be used to target potential ID theft victims. As the profiles reveal much information about habits and preferences of the profiled individual, they may reveal attributes of interest to perpetrators. For instance, if an individual's restaurant preferences (as described in section 6.3.2) include high-class restaurants, as well as other expensive habits, this may signal that this individual is

[25] See Bohn et al. 2004, p. 9-14 for an interesting analysis of privacy issues.
[26] See section 7.1.3.2.B.1 and C, section 7.1.3.4.A and B on the use of technology and 'ambient' law to solve some of these problems.
[27] Interestlingly the public's awareness of the volume of ID-theft has remarkably increased since the California Security Breach Notice law - in effect since 2003 - requires firms to notify their clients when confidential personal information has been breached.

wealthy. And this in turn may make this individual a suitable target for identity fraudsters. Of course positioning oneself close to or inside such restaurants to register clients will reveal the same information. But again, as the AmI scenario is based on RF communication, the electronic monitoring of profiles is less obtrusive than spying on clients from the next table. Once a potential victim is targeted, the fraudster may try to acquire the required PII by means of hacking the victim's IMD, but also monitoring and surveillance, and 'traditional' tools of the ID crime trade, such as phishing can be used to lure the victim in revealing his PII.

6 End user Control: Privacy and Mobility

6.1 Two reasons for end user control

In FIDIS deliverable 7.2, profiling is described as a tool used by service providers (group profiling at the level of the AmI environment), whereas the data subject or end user seems to have little control over the construction and the use of those (group) profiles. In this section we will discuss attempts to develop technologies to redirect the control over profiles to the end users. There are two reasons to emphasise end user control in relation to ambient intelligence:

1. To begin with - like in the case of any other type of profiling - some of the privacy and security risks discussed in chapter 5 could be mitigated by means of end user control (use of partial profiles (pseudonyms) and/or local storage of personal information).

2. A second reason for end user control by means of local storage of the personal profile is that it would allow a person to move from one AmI environment into another, without the need to build up a personal profile all over again. Below we will work out two scenarios that could facilitate such local storage. Of course the more commonly envisioned option to achieve the same goal is the construction of a networked environment that makes different environments interoperable without access to data stored on the personal digital assistant of the end user. According to the ISTAG report of 2003 'AmI cannot be achieved piecemeal: it requires coherent application of resources European wide'. The scenarios worked out below seem to indicate otherwise.

6.2 Privacy Enhanced Ambient Intelligence Profiling

6.2.1 Context

Contrary to the example of the Smart Home, we now focus on contexts that are not trusted for the user. That is, we do not consider a domestic network here given that the data gathered by sensors or devices in the home environment may be controlled by a home (trusted) computer, and is therefore under the control of the user. Rather, the techniques proposed here could be used for interacting with devices located outside the personal sphere (e.g., public spaces, pubs, stores, offices, etc.).

We consider two different sorts of AmI devices: High power and low power. In the next two sections, we present the technologies that can be implemented for these two types of devices. Although the techniques are radically different, they both share a common requirement: The user must have an identity management device with sufficient storage capacity and computing power to perform the protocols and build profiles.

The burden of the personal data management is at the user side. Note that in such a model, large databases which store the data of all users are no longer needed, as data is stored in a distributed form, i.e., each user must take care of his own data.

We consider a model in which the user has a powerful identity management device, and interacts with untrusted devices.

6.2.2 Anonymous credentials

Anonymous credentials are a powerful identity management technique with strong privacy and security features. One of the systems that implement these credentials is 'Idemix', which has been explained in detail in FIDIS deliverable 3.3. Here, we give a brief summary of this system in order to indicate its possible uses in certain ambient intelligence contexts.

Anonymous credential protocols require costly operations, and can only be performed by devices with high computing power. Many ambient intelligence contexts may therefore not be suited to implement this technology. Anonymous credentials work as follows: users may establish unlinkable pseudonyms with different organisations (in this context, these organisations are the ones providing the ambient intelligence services), obtain credentials signed by these organisations certifying certain attributes, and prove these attributes to verifying devices.

By using this system, users have control on their identity attributes. They can choose which attributes they want to show or prove to a certain device. The system allows for minimal data leakage, as well as for pseudonymous identity management. It also implements accountability mechanisms, allowing for de-anonymisation under certain conditions.

Such a system should be implemented in the contexts in which the user wishes to maintain a permanent pseudonymous identity, and for access control purposes. For example, it could be used in order to grant access to certain buildings or rooms (the user should prove that he is authorised to access the resource). These credentials can also be used to implement secure anonymous electronic cash payments for small purchases.

6.2.3 Dynamic user-generated profiles

Many ambient intelligence devices are designed to provide the user with a customised service, by taking into account the user's preferences. One possibility is to implement such a system by identifying the users and maintaining internal information about their behaviour and preferences. In this scheme, the data of all users must be kept in a database, accessible to devices.

Such a system collects personal information on users in a way these cannot control. From a privacy perspective, it would be desirable that users have control over their own personal data. We propose a system in which the behavioural data of the user is kept in the user IMD. When the user interacts with a device, the IMD provides the preferences of the user for the particular service the device is providing. If there is any feedback information extracted by the behaviour of the user, it is transferred by the ambient intelligence device to the IMD, so it can update the internal information of the user for later transactions.

The IMD builds the preferences presented to the device according to the previous behaviour of its owner. Users who have the same preferences for a service will appear as the same user to the device. If a user changes his behaviour of preferences, it will appear as different from previous transactions to the device. Note that, in this scheme, IMDs do not identify themselves, and the *profiles* presented do not contain a unique identifier.

Let us illustrate this system with an example. Consider a coffee machine that is equipped with an ambient intelligence device. When users want to get a cup of coffee, the machine must be able to produce the coffee according to the taste of the user (strong, weak, big, small, with or

without milk, with or without sugar, etc.). The user sets in the IMD his profile or preferences for the coffee machine.

If dynamic user-generated profiles are implemented, the IMD contacts the machine and orders a coffee with the given set of preferences (e.g., strong, small, without milk and with sugar). The coffee machine is unable to distinguish between two users who like coffee the same way, as the preferences showed by the IMD are identical. Note that the IMD does not present a unique identifier for the user. If for example, a user goes on diet and decides to skip sugar, the preferences change in the IMD, and the user appears as different from previous times to the coffee machine.

This technique has been proposed for targeted advertising, given that the advertisements are more effective if selected according to the preferences of the user. As ambient intelligence also works on profiles and preferences, the technique can be adapted to this context.

6.3 The tension between end user control and an intelligent environment

6.3.1 Two types of end user control

End user control can take shape in two forms:

1. The end user constructs her own profile (data set) as input into her personal digital assistant (PDA) that is used as a privacy enhanced identity management device (IDM). Depending on the way the IMD is programmed, information is communicated to a specific environment. This environment can read the information and match it with its own predefined profile (data set), after which action will or will not be taken. In this case the profiles involved are not the result of profiling technologies, forming simple data sets.

2. The end user does not create predefined profiles, but allows itself to be profiled by intelligent device in the environment. However the profiles that are constructed are stored in the PDA of the data subject, thus creating a dynamic profile in the course of time. Neither behavioural data, nor the profile itself are stored at the level of the intelligent device in the environment (so, not at the level of the data controller, not at the level of the service provider), expect if permission is granted by the data subject (a decision that can be delegated for trusted environments to the PDA). In this case the profiles involved are the result of profiling technologies, forming correlated data sets.

The case study below will illustrate the use of both types of profiles.

6.3.2 Case study of end user control: Ronny goes to Tokyo

This example gives a view of a possible application of AmI and the tension between end-user control and AmI environment control. The interaction between data subject and the environment is supported by a Personal Digital Assistant (PDA) that facilitates privacy and identity management by the end-user; Location Based Services (LBS); wireless communication, and a database containing addresses, opening hours and menus of restaurants.

Ronny stays - for the first time - in Tokyo, to attend a workshop. He invites a colleague from Croatia to have dinner after the workshop. He needs to take a quick decision where to go and

needs to know the restaurants that meet his preferences. Instead of wondering around without knowing where to go, he uses his PDA that contains his preferences for restaurants (see Figure 6).

His personal profile contains the following preferences: anonymity, classical music, diet food, local food, medium prices. The PDA sends a request to a database, containing a list of restaurants, with the opening hours and the characteristics of the restaurants.

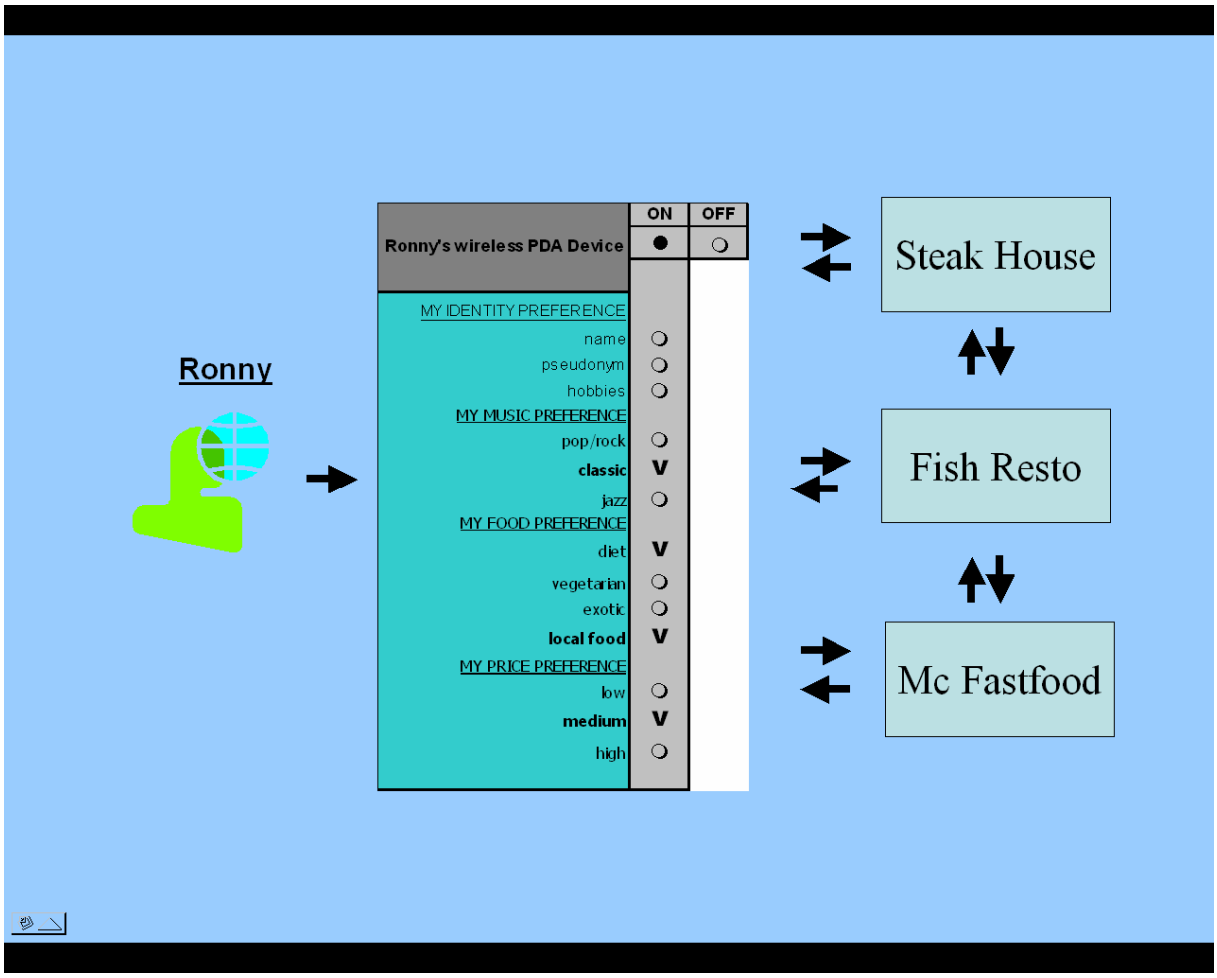


Figure 6: Ronny's PDA - communicating with restaurants in Tokyo.

The first restaurant, a steak house, plays rock music, has no diet menu and is medium- priced. The second restaurant is a local fish restaurant which offers diet menus and plays classical music. The prices are medium. The third restaurant is a fast-food chain that does offer diet menus and contains low prices. All restaurants are open at the day of request. The database receives the request, takes into account the opening hours of the restaurants and matches the restaurants' data with Ronny's preferences. Consequently, the contact address and location of '*Fish Resto*' is displayed on the PDA of Ronny. He can make an immediate reservation. The preferences on his PDA form a profile that is communicated to his AmI environment. The restaurants themselves also use profiles. All persons that meet the requirements of such a profile are allowed to display the restaurant on the PDA. The restaurants that created a profile (data set) for clients that are willing to pay high prices, are not interested in Ronny who chooses medium priced restaurants.

In the case described so far, profiles are used that have nothing to do with profiling technologies. We are dealing with pre-defined input from the end-user and pre-defined input from the service provider. One could of course claim that this is not an example of ambient intelligence, but rather of ubiquitous computing. The environment is not learning, but just following predefined input.

We can introduce software intelligence into this example by allowing the PDA and/or the devices of the service provider to record and process the actual behaviour of Ronny: how often he goes to which type of restaurant; which wines he chooses; whether he takes an entrée, a dessert; how far he likes to walk or travel from his hotel; whether he likes to meet new people, share dinner with other congress- participants or rather eat alone; how he takes his after dinner coffee; what time he gets home. This and other information may not be relevant immediately but could be built into a complex profile, stored on his PDA, accessible at different levels by different types of service providers. It could mean that fewer restaurants are displayed because the profile will be fine- tuned to a lot of different factors, matching with greater precision the offers of neighbouring restaurants. It could even be that those restaurants that do not present recently updated profiles with detailed information are discarded right away. (Of course Ronny may eventually come to live a rather boring kind of life, walking around in a world that satisfies his preferences - little chance of surprise.) To maintain end-user control all data collected and profiles constructed by the intelligent devices in the AmI environment should be stored on Ronny's PDA - with the guarantee that they will not be stored with the service provider. The interesting question would be whether the same level of intelligence can be reached if only the PDA of the end user is able to construct profiles.

7 Legal issues

7.1 Introduction

In FIDIS deliverable 7.2, the concept of group profiling has been described as the process of constructing profiles (correlated data), that identify and represent a group/category/cluster.

The application of a group profile is described as the identification and representation of a person as a member of a specific group/category/cluster. Identification in this case does not mean discriminating a person *from* all other persons, but rather focuses on identifying a person *with* (as part of) *a certain group/category/cluster of persons*.

In the case that a group profile is applied to a member of the group, this group profile can either be applied to an identifiable person, or - in the case of anonymity or pseudonymity - to a non-identifiable person.

Personalised profiling is described as the process of constructing profiles (correlated data) that identify and represent a person. When applied, the profile identifies and represents a person as a specific person. The set of correlated data that identify and represent a person as this specific person does not imply that the person is identifiable in the sense of a unique identifier. If the person uses pseudonyms, he or she can be identified as the same person per context, without necessarily linking this specific person to the physical person.

In this chapter, we will pay special attention to group profiling since there is some legal uncertainty regarding the applicability of data protection legislation that is only applicable to personal data relating to identified or identifiable natural persons. As will be indicated, even though personalised profiling seems to fall within the scope of data protection legislation by its very nature, it is still possible to make personalised profiles without identifying the person in the sense of the directive.

The legal analysis in this chapter will be built upon the different steps that can be differentiated in the construction and the application of profiles. Each step will be subject to an analysis of laws and regulations on the EU level. The described laws and regulations are not only privacy and data protection law, but also others such as e-commerce and consumer protection law. These laws contain provisions that may be applicable to profiling in AmI.

The three steps of profiling that we follow are:

1. The *collection* of personal data and of other information to construct the (group) profile. With collection we also mean the storage and aggregation, i.e. the systematic storage and re-organisation of personal data and of other information to make the data and information accessible (section 7.1.1)
2. The *construction* of (group) profiles, including making the personal data anonymous (section 7.2).
3. The *application* of the (group) profile in an AmI environment (section 7.3).

7.1.1 The first step: collection of personal data and other information

7.1.2 The collection of information, other than personal data

Any information can be used to construct profiles. Weather reports, environmental data, context, statistics, economical fluctuations, time, date, location of the AmI environment, do not fall within data protection law, as they do not relate to an identified or identifiable natural person (Data Protection Directive 95/46, article 2.a). Most of this information belongs to mankind and is part of our *public domain*, to use a term often used in copyright law.

The collector and/or processor of these data however, has to take into account that intellectual property rights may be at stake in case the information is part of a database or in case it is described or arranged in an original way such that it falls under copyright. Even the methods to collect information (and to process it in an intelligent way) may be an object of software patents or patented business models. In all these cases, when intellectual property rights on the data or on the databases exist, the collector must obtain a licence to use the data or the database. We will not further discuss the difficult issue of intellectual property law at this point in order to focus on the collection of personal data.

7.1.3 The collection of personal data

Personal data form the *corner stone* for profiling in AmI environments. Two things should be questioned: First, what are personal data and second, when does data protection law apply to the collection of personal data to construct a profile. The legal basis for personal data protection in the EU can be found, mainly, in two directives: Data Protection Directive 95/46 and Directive 2002/58 on Privacy and Electronic Communications.

7.1.3.1 What are personal data and when is data protection law applicable?

Personal data are defined in the Data Protection Directive 95/46 as "any information relating to an identified or identifiable natural person ('data subject')". An identifiable natural person is "one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"(article 2.a.). Following the *preamble* of the directive, to determine whether a person is identifiable or not, "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person" (considerans 26). In other words, the directive only does not apply in cases where *no reasonable possibility exists of linking* the personal data to an identified person.

Personal data are amongst others: one's name, address and ip-address, phone number, number plate of a car, DNA, location, picture, telecommunication data, shopping record, etc. as far as the data can be linked directly or indirectly to an individual. The IP-address and mobile phone number can be linked with the user who is often the subscriber.[28]

It is legally seen not relevant who can identify the data subject directly or indirectly (the data controller or another person) neither at what moment data subjects can be identified directly or indirectly (instantly or later). Two important questions arise.

[28] In cases when the user is not the subscriber, which happens often in employer-employee situations, the possibility to identify the user (the identifiable person), remains. That is why the personal data protection directive also applies to mobile phone communications by subscribers that are legal persons (companies).

First, what if the data of persons are collected, *while they cannot be linked to an individual*? It can be the case when e.g. presence only is detected, or length or weight is measured, or when the movements of people in a supermarket are monitored. This can occur when RFID tags are integrated in shopping trolleys. By collecting these anonymous data, profiles of shopping people can be built.

Second, *when does the directive apply and when is it not applicable?* The legal definition of personal data must be read together with other provisions in the directive that exclude the application of the directive in some particular situations when personal data are collected, namely the collection of data

(1) concerning *legal persons (this follows from article 2 that restricts the application to data relating to natural persons)*;

(2) carried out by a natural person in the exercise of activities which are *purely*[29] *personal or domestic*, such as correspondence and the holding of records of addresses (article 3 par. 2);

(3) carried out for the purposes of *public security*, *defence*, *national security* or in the course of State activities in areas of criminal law and other activities which do not come within the scope of Community law (article 3 par. 2);

(4) rendered *anonymous* in such a way that the data subject is no longer identifiable (article 2, read together with considerans 26).

This is obviously of importance for the applicability of the directive on profiling practices because many group profiles can be built upon anonymous data. Constructors of group profiles are often not interested in a particular individual and do not need to process personal data that identify or can identify a particular individual. Often, identifiable characteristic(s) of an unidentifiable person can be of more value than the identified person itself.

However, a combination of several anonymous data could make a person identifiable at the end of the day. This implies that all data collection and processing may eventually lead to the possible identification of a person. This could mean that, with hindsight, the directive should be applicable. At this moment it is still unclear how the courts will interpret the directive on this point.

If anonymous data are valuable for the construction of group profiles and if identifiable characteristics can be even more important than identifiable persons, we can conclude that AmI environments that make use of group profiles do not need to identify persons. In that case the data protection directive will probably not be applicable. This would mean that natural persons will have no right or claims on the basis of the data protection directive to prevent group profiling. This has as a consequence that a subject has no control over the construction of group profiles that may (at a later stage) concern him of her.

[29] In considerans 12, the word *exclusively* is used for the word "purely". For the purpose of this chapter, personal activities and connected homes do NOT fall under this exemption.

7.1.3.2 The principles, rights and obligations of data protection law

The basic principles of data protection legislation are spelled out in international texts from OECD, Council of Europe, UN and the E.U. Each of these organisations produced classic basic data protection instruments, respectively the OECD Guidelines[30], the Treaty 108[31], the UN Guidelines[32] and the Data Protection Directives. The EU also included the right to data protection in the European Charter of Fundamental Rights.[33]

EU Data Protection Directive 95/46 aims to reconcile the free flow of personal data between the Member States with the protection of fundamental rights and freedoms of individuals, notably the right to privacy with regard to the processing of such data. It contains the main principles that relate to data protection. The principles are implemented by two types of legal tools: Obligations for data controllers on the one hand and rights conferred to the individuals on the other hand.[34]

7.1.3.2.A. The obligations of the data controller

7.1.3.2.A.1. The fairness principle

Any processing of personal data must be lawful and fair to the individuals concerned (article 6.1.a). This fairness principle is abstract and difficult to evaluate. In legal theory we refer to the 'abstractness' of this kind of principles as 'open texture', indicating the impossibility and undesirability of rigid and detailed articulation of concepts and principles that anticipate a host of indeterminate future events. The question is not whether group or individual profiling *as such* infringes the fairness principle. A lot will depend on the particular context of each case and on the checks and balances built into the actual practice, that should allow stakeholders (like the data subjects) enough bargaining power within the process of collecting and processing of personal data.

7.1.3.2.A.2. The obligation to inform

The right to be informed about data collection will be discussed in the section on the rights of the data subject. However, as it is not literally included in the articles of the directive this right is more or less inferred from the obligations of the data controller to give information to the data subject (article 10 and 11 of D95/46 EU). It can also not be deduced from the right to give consent (see *infra*), because the individual's explicit consent must not be obtained in all circumstances. Consent is for example not needed when the collection is necessary to protect

---

[30] Cf. OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 September 1980 in *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, OECD, 1980, 9-12; *International Legal Materials*, 1981, I, 317.

[31] Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981, *European Treaty Series*, no. 108; *International Legal Materials*, 1981, I, 422.

[32] The *United Nations Guidelines* are a more recent international instrument: Guidelines concerning computerised personal data files, adopted by the General Assembly on 14 December 1990. We will not further discuss these UN Guidelines, because in Europe they are overshadowed by the other regulations.

[33] Charter of Fundamental Rights of 7 December 2000 of the European Union, *Official Journal of the European Communities*, C 364, 2000, 1, entered into force 7 December 2000.

[34] Apart from these two implementations the Directive also creates obligations for Member States to establish a national supervising authority (D95/46 EU, article 28). Such a system is absent in e.g. US jurisdiction.

the vital interests of the data subject (article7.d.) or when the processing is necessary for the performance of a contract to which the data subject is party (article8.7.b.).

Section IV of the directive implicitly refers to a right to be informed by indicating the kind of "information to be given to the data subject" in case of data collection. This would imply that data subjects have to be informed every time their data are collected. This raises interesting issues in the context of AmI, as in a networked environment envisioned by the AmI vision, data are collected continuously and everywhere. Does it mean that the data subject must be informed constantly? If so, law could be a difficult partner for AmI in a vision that presumes an environment that automatically adapts to the inferred user's preferences.

As a solution, one could argue that data subjects should *reasonably expect* that their personal data will be collected and processed in certain circumstances, e.g. with camera surveillance in public places. Still the right to be informed remains important in sensor networks (a kind of Ami environment), as it relates to *informational self-determination.* A subject should have the right to know whether services offered, are the product or consequence of profiling practices. If this right does not exist, we cannot detect what motivates our service providers, and - in the end - we cannot check to what extent they profile us to adapt to our preferences and to what extent they adapt us to their preferences.

This problem could maybe be tackled by attributing a right to anonymity:[35] the data subject should always have the right (and therefore the technological possibility) to be anonymous and to not to be subject to personal data collection, for example by switching off his online communication device in order to remain in his private offline sphere. [36] However, the right to anonymity does not solve the problem completely because the collection of identified characteristics from anonymous people may still lead to a loss of self-determination.

One way to increase legal certainty would be to legislate that when the data subject's online communicator (a mobile phone, an interactive television set, a car, …) is switched on, data procession can take place without notification. This would render explicit and define the reasonable expectation of data processing in data protection legislation.

This last solution only applies to communications between personal digital devices and AmI environments. It does not stop AmI environments from collecting data by means of sensors, as such data flows cannot be switched off by the data subject. Consequently, subjects may also want to have the right to pull the plug out of the AmI environment(s) itself. This is however not possible in *public* AmI environments.[37]

7.1.3.2.A.3. The purpose specification principle (finality principle)

Article 6.1.b. states that personal data must be *"collected for specified, explicit and legitimate purposes and may not [be] further processed in a way incompatible with those purposes."*

---

[35] See Recommendation 3/97 on Anonymity on the Internet, Adopted by the article 29 Working Party on 3 December 1997.

[36] This private offline sphere should be available at any chosen time and place and is therefore not necessarily limited to a private physical place as we know it today, such as the private home or the public toilet. We could speak of "digital private territories". See the short text "Digital Territories: Bubbles", available on http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf (the text is a draft for "Vision Book Project", of which abstracts are available at
http://europa.eu.int/information_society/topics/research/visionbook/themes/index_en.htm.

[37] We can conclude that these problems bring us to the discussion whether a person has the right not to be subject to an AmI environment.

But article 6.1.b. continues: "*Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards"*.

These safeguards "*must in particular rule out the use of the data in support of measures or decisions regarding any particular individual"* (considerans 29). [38][39] Considerans 26 states, "*the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable"*.

This seems to imply that the data collector is not obliged to specify the profiling purpose in case of anonymised data. However, several situations can be anticipated:

- If the data are collected anonymously from the beginning (the data can not be linked anymore with an identifiable natural person), data protection law seems not to apply, so the data collector is not obliged to specify the profiling purpose.
- If the data are not collected anonymously (the data can be linked with an identifiable person), data protection law applies (definition of personal data).

Four different situations can indeed occur:

1. The personal data of identifiable persons are collected for profiling purposes only and they are not made anonymous.
2. The personal data of identifiable persons are collected for profiling purposes only and they are made anonymous.
3. The personal data of identifiable persons are collected in first instance for other purposes and they are afterwards also used for profiling purposes, and they were not made anonymous.
4. The personal data of identifiable persons are collected in first instance for other purposes and they are afterwards also used to construct profiles, and they were made anonymous.

Case (1) seems to imply that the purpose has to be specified because data collection is taking place only for the purpose of profiling. Restrictively interpreted, article 6.1.b.only applies to "*further processing of data for historical, statistical or scientific purposes"*. When the only purpose of the data collection is statistical, there is no situation of "further" processing of personal data.

In the second case the situation is more complex because we are confronted with considerans 26 stating, "that the principles of protection shall not apply to data *rendered* anonymous in such a way that the data subject is *no longer* identifiable". One could argue that the purpose has to be specified for two reasons: First, article 6.1.b.only applies to "*further processing of data for historical, statistical or scientific purposes"* and second, the purpose specification

[38] While on the one hand it is not clear whether profiling would fall within the scope of 'statistics', on the other hand the text recognises that statistics can be used to support measures or decisions regarding particular individuals. Since profiling involves mathematical techniques like statistics, we will suppose that profiling falls within the scope of 'statistics'.

[39] It is important to underline that the text states that the data are not used for taking measures or decisions regarding any particular individual; the restriction would thus regard not only data subjects whose data are processed, but any particular individual subject to measures or decisions based on the use of statistical techniques.

principle does not apply *from the moment that the data are rendered anonymous.* In other words, it does apply at the moment of collection.

In situation (3) we also think that the profiling purpose has to be specified when reading article 6.1.b. in combination with considerans 29: "*Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual"*. When the statistics are profiles and these profiles are used as group profiles, they can be used to support measures or decisions regarding any particular individual. The word "any" particular individual is of importance, because group profiles do apply to any individual, belonging to a group. When my data are used to build group profiles and the group profile is applied to another individual, one could speak of a measure or decision regarding any particular individual.

Also in situation (4), the purpose has to be specified for the same reasons as in situation (3).

We can conclude that the purpose of constructing group profiles does not have to be specified when no personal data are collected. If personal data are collected and they are used for profiling purposes, this purpose has to be specified in as far as it aims for more than just statistics: as soon as it supports measures and decisions towards at least one particular individual the purpose of profiling should be specified. We would like to note that, even if the purpose of profiling has to be specified, the purposes are often too broadly or not understandably described in the general terms and conditions of the service provider. Also, an effective control on the principle of finality, e.g. by supervisory authorities, does not really exist. Another problem is that most of the time the data subject does not know what data is being processed, whether legally or illegally. In that case one cannot expect the data subject to claim that his data have been collected and processed for purposes that are incompatible with the Directive.

7.1.3.2.A.4. The proportionality principle

This principle states that the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (article 6.1.c). It again has an open texture (its meaning cannot be defined out of context). What is non-proportional data collection in the case of group or individual profiling? We are confronted with many subjects having an interest in their data being collected and processed extensively during their lifetime. A 'vast collection of processed data' can be very useful to build personal profiles, to create enhanced personal agents. The more relevant data the intelligent environment and/or personal agent collect and process, the more services and environments can be adapted to the user.

Compliance with this principle is also difficult to enforce. So far this principle is hardly supported by technology, because the collection, storage and procession mainly depend on the data controller that establishes type 1 identity management systems (account management systems, as discussed in FIDIS deliverable 3.1). Widespread use of type 3 identity management devices (privacy enhanced personal digital assistants) could change this situation by redirecting control to the end user. So the question is whether today's legislation offers enough protection: Should we respect its open texture and define what is proportional at the level of technology? If this takes away the citizen's right to decide autonomously whether and to what extent her personal data can be used for profiling, the right to privacy and autonomy is clearly at stake. Insofar as a disproportional data- collection should be prohibited, even if

consent has been given, legal support could be created in consumer protection law, stating e.g. that personal data may not be exchanged ('traded') for price reductions.

7.1.3.2.A.5. The consent principle

According to article 7, to be legitimate, the processing of personal data may only take place if the data subject has unambiguously given his consent or if the processing is necessary for:

1. the performance of a contract to which the data subject is party, or for taking steps at the request of the data subject prior to entering into a contract, or
2. compliance with a legal obligation to which the controller is subject, or
3. protecting the vital interests of the data subject, or
4. the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, or
5. the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

The *consent principle* of article 7 is a corner stone for data protection. Consent by the data subject is defined as "any freely given, specific, and informed indication of his wishes" (article 2.h). Consent for the collection of data that are not sensitive, may be given orally. In the case of collecting and processing of sensitive data, the consent given must be explicit (article 8 - 2.a).[40] Especially the last condition of article 7[41] seems to give a free way to data controllers to collect personal data without consent. The question is who determines when data collection for the purpose of profiling is in fact necessary for the legitimate interest of the data controller or a third party. If we combine the fact that - in practice - most of the time data subjects do not know that or which data are collected with the fact that consent is not necessary if profiling is necessary to pursue legitimate interests, then we may infer that in the end the data controller will decide about this necessity.

7.1.3.2.A.6. Confidentiality and Security

The security obligations require that appropriate technical and organisational measures are taken both at the time of the design of the system and at the time of the processing of the personal data itself (article 17 D95/46 EU).

[40] As an example of this additional condition for sensitive data, the word 'explicit' has been translated into 'in written' in the Belgian data protection act that implemented the directive. Many other countries require explicit instead of specific consent.

[41] No consent is required if the processing is "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."

Also, an appropriate level of confidentiality and security must be implemented, taking into account the state of the art and the costs of the implementation of the measures in relation to the risks represented by the processing and the nature of the data to be protected (see article 16 & 17). AmI environments require interconnectivity and interoperability through different networks and different controllers, located in different countries. It will be difficult to find out who is responsible in case of a technical or organisational failure. It is very difficult to trace back at what point data are stolen of illegally disseminated to third parties, and so far it is in fact rather difficult to even know at all that there has been a security or confidentiality breach.[42] The provisions may again seem vague or abstract, as they refer to circumstances that will vary depending on the context and can only be defined on a case-by-case basis. The reference to the state of the art in combination with the costs of implementation could make this type of protection dependent on the accepted standards in the relevant sector.

7.1.3.2.A.7. Notification to the supervisory authority (article 18)

The transparency of personal data processing is a key notion of data protection law. Notification to the supervisory authority is designed to ensure disclosure of the purposes and main features of any processing operation in order to verify that the operation is in accordance with the national implementation of the directive. It is also designed to know who collects data. The information to be given in the notification must includes among others name and address of the controller, purpose(s) of the processing, categories of data subjects and categories of data processed, categories of recipients to whom the data *might* be disclosed. Most of this information must be published in a public register. This public register may be inspected by any person but hardly helps individuals to control the constructions of profiles.

Many standard types of data processing are exempted from notification in the national laws of Member States. Also, the public register does not allow the user to know which persons or companies in fact posses, use or process his personal data, because only *categories of subjects* (and not the subjects themselves), only *categories* of data (and not the data themselves) and only the *categories* of recipients (and not the recipients themselves) to whom the data might be disclosed, are indicated in the notification.[43]

7.1.3.2.A.8. Sensitive Data

Processing of so-called *sensitive* data[44] is prohibited, unless the data subject has given explicit consent or other conditions such as the vital interest of the data subject are fulfilled (article 8).

The list of sensitive data is a restrictive list. In an AmI world, any kind of data could become sensitive: Your food purchases may provide information concerning your health or religious

---

[42] In the US, legislation and practice guidelines are well under way and already partly implemented, see http://www.privacy.ca.gov/recommendations/secbreach.pdf, p. 7 and 23-26 for the 'California Law on Notice of Security Breach', see the proposal for a US Federal 'Personal Data Privacy and Security Act of 2005' at http://www.bespacific.com/mt/archives/008576.html, and the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* at http://www.fdic.gov/news/news/financial/2005/fil2705a.html.

[43] However, this notification of *categories* of data, processions and recipients might be, on the other hand, a very good solution because a notification of personal data would create an enormous, centralised database in which all kinds of information can be found and with which the most advanced group and personal profiles could be built…

[44] "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life"

belief ; when you program your PDA to look for single people in the neighbourhood, it may provide sexual preferences etc. In fact, profiling enables 'masking'. 'Masking' is a practice whereby data that is in itself insignificant, is correlated with sensitive information. By using the insignificant information, the protection of sensitive data can be avoided.

7.1.3.2.B. Rights conferred to individuals

7.1.3.2.B.1. The right to be informed

The right to be informed exists in the obligation of the controller to provide data subjects with the identity of the controller (and of his representative) and the purposes of the processing for which the data are intended. *If necessary to guarantee a fair processing,* the data subject must also be provided with: the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, the possible consequences of failure to reply and the existence of the right of access to and the right to rectify the data concerning him (article 10).

When the data have not been obtained from the data subject himself but from a third party, the controller or his representative must at the time of recording the personal data or, if disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the data subject with information as described above, including the indication of categories of data concerned (article 11).

At this point we will give attention to this information procedure *as such* because AmI should somehow also be based on what we can tentatively call 'ambient law'. Obviously one cannot imagine an automated AmI world where the law obliges data controllers to continuously present the information on the purpose of data collection information to individual users. Such purpose specification would put too much of a burden on both the data subject and the data controller. Thinking of user convenience, this would create an overload of information, whereas AmI and profiles are in fact designed to limit the information stream towards an individual.

The information procedure of article 10 reflects a kind of *formalisation* of the data collection and processing procedures. It aims at making the data collection both legal and legitimate without however really informing the individual. If information on the purpose is available, the data subject will most often not have the time to read it or may not understand the privacy disclaimer. As mentioned, a purpose can be described in general terms such that *any* specific purpose will fall within its scope. And in most cases, the privacy disclaimer is written in the language of the place of data collection, which is not necessarily a language understood by the data subject. What is needed is a balance between the fact that the information targeted at the data subject should be as limited as possible to enhance the user's comfort and the user's interest to be informed of the purposes of the collection and processing. One could think of legislation and technology that keep this information "ambient" by obliging AmI service providers to supply the purpose information in such a format so that the intelligent agent of the user can recognise the purposes independently and take decisions according to the user's preferences. A user could instruct his personal agent to automatically allow certain categories of purposes, while disallowing other specific categories. On top of that the PDA can signal the user if the information falls outside the scope of both, in which case the data subject can decide himself. This could shift the balance of power from the data controller towards the consumer. It could also allow the user to define when and to what extent his data can be made anonymous by the data controller in order to construct group profiles.

7.1.3.2.B.2. The right to consult the data (right to access and individual participation)

The data subject has the right to obtain from the controller (1) communication to him in an intelligible form of the data undergoing processing and of any available information as to their source; (2) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15.1 (article 12).

7.1.3.2.B.3. The right to request corrections

The right to request corrections is important to avoid possible mistakes in profiles based on data that are not correct or not up to date. To request these corrections, the data subject should have access to his data and therefore, first needs to be aware who is holding the data where. Today, this has become an impossible task due to the proliferation of data sharing, transfers and dissemination to third parties.

One possibility to remedy this situation could be to tag personal data with digital rights management (e.g. adding a hash code to the data), but this seems technologically not possible because the DRM functionalities in the data seem to require much more bits and bytes than the personal datum itself. It could be applied to data such as pictures that are built of many bits and bytes. Another possibility could exist in the obligation for data collectors to send a copy to the data subject each time when data are collected, so that the subject has the possibility to contact every data collector to request a change of the data. This would require almost 100% compatibility and interoperability of personal data tools, devices and databases.

7.1.3.2.B.4. The right to object to the processing in certain circumstances

The data subject has the right to object at any time to the processing of data relating to him at least in the following three situations (article 14): (1) when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; (2) when processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed. However, save when otherwise provided by national law, the data subject can only object to processing of data concerning him in these first two situations when he gives proof of a justified objection, an objection "on compelling legitimate grounds relating to his particular situation", and (3) when the controller anticipates personal data being processed for the purposes of direct marketing.

It is not clear today if the provision of goods and services is included in direct marketing. Is direct marketing only understood as the "promotion" of goods and services, or does it also apply to the delivery of goods and services itself? And secondly, if this is the case, does the right to object only apply if the provision of goods and services is commercial? The difference between group and personal profiling could be relevant here. There are arguments to claim that personalised profiling enables "direct" marketing ("direct" here meaning directly towards a particular individual) while group profiling does not necessarily enable such direct marketing. On the other hand, when a group profile is applied, this will affect the person targeted, even if the marketing is directed towards a category of persons.

7.1.3.3 Privacy and Electronic Communications Directive 2002/58

The Privacy and Electronic Communications Directive[45] states in its preamble (considerans 30) "systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required".

This directive does not only offer protection to natural persons; also legal persons enjoy the attributed rights (article 1.2.). The directive distinguishes traffic data and location data in electronic communications (article 2).[46] It contains provisions on security and confidentiality of the electronic communication services (and networks).[47] It also refers explicitly to cookies and related technologies. Cookies are a powerful tool to track, monitor and profile people.

7.1.3.3.A. Traffic data

The level of protection accorded to a natural or legal person's traffic data depends on the purpose of the processing: (1) *transmission* of communication, (2) *billing* and (3) *marketing* of electronic communication as well as *providing of value added services,* e.g., tourist information, route guidance, traffic information and weather forecasts.

- For the purpose of the *transmission* of a communication, traffic data relating to subscribers and users may be processed and stored by the service or network provider but must be erased or made anonymous when it is no longer needed for the purpose of the transmission (article 6.1.). The obligation to erase or anonymise traffic data does not conflict with procedures such as caching or using login information for access control (considerans 28).
- Traffic data, necessary for the purposes of subscriber *billing* and interconnection payments, may be processed and stored up to the end of the period during which the bill may lawfully be challenged or payment pursued (article 6.2.).
- Traffic data, necessary for the purpose of *marketing* electronic communications services or for the provision of *value added services*, may be processed by the service provider to the extent and for the duration necessary for such marketing or services, if the subscriber or user to whom the data relate, *has given his consent* after he has been informed about the type of traffic data processed, the purposes and the duration of the processing. Users/subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time (article 6.3.).

---

[45] Directive 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *Official Journal L 201,* 31/07/2002 P. 0037-0047.

[46] Article 2 defines traffic data as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof", and location data as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service". According to considerans 14, location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

[47] Article 4 & 5.

In any of these cases, processing of traffic data must be restricted to what is necessary for the purposes of such activities and must be restricted to persons acting under the authority of the network or service provider. In any of these cases, if data are processed for a longer time than for the transmission, the user or subscriber must be informed of the duration of such processing.[48]

7.1.3.3.B. Location data

Location data other than traffic data are data that "indicate the geographical position of the user without being processed for the purpose of the conveyance of an electronic communication or the billing thereof". (1) Such data may only be processed (a) when they are made anonymous or (b) with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a *value added service (article 9.1.)*.

When consent must be obtained, the service provider must - prior to obtaining the consent - inform the users or subscribers of (a) the type of location data other than traffic data which will be processed, (b) the purposes of the processing, (c) the duration of the processing and (d) whether the data will be transmitted to a third party for the purpose of providing the value added service. When consent has been obtained, the user or the subscriber (a) shall be given the possibility to *withdraw his consent* for the processing of location data other than traffic data at any time and (b) must continue to have the possibility, using a simple means and free of charge, of *temporarily refusing* the processing of such data for each connection to the network or for each transmission of a communication (article 9).

7.1.3.3.C. Cookies and related programs

Cookies are often used to implicitly collect personal data. However, the Privacy and Electronic Communications Directive states explicitly that users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment (considerans 25). This is particularly important where users other than the original user have access to the terminal equipment.

Information and the right to refuse information may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user- friendly as possible. Access to specific website content may still be made conditional on the well- informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.[49]

7.1.3.4 E-commerce and Consumer Protection Law

As we have seen, data protection law does not always apply in the case of profiling practises. In the case of the collection of data that are not linkable to identifiable persons; in the case that data are used to construct a group profile and when the profile is applied to an

[48] If a Framework Decision on Data Retention comes into force, the protection guaranteed by this Directive will diminish substantially, see http://www.edri.org/issues/privacy/dataretention .

[49] See Ranse, Stéphanie, 'Le profiling des internautes au regards du droit au respect de a vie privée: le coût de l'efficacité!', *Revue du Droit des Technologies de l'Information*, n° 20/2004, 37-58.

anonymous user in a group, D95/46 may not be applicable. This can lead to a loss of control and creates questions as to autonomy and self-determination. We shall now investigate possible protection offered in the field of e-commerce and consumer protection law.

7.1.3.4.A. Directive 93/13 on unfair terms in consumer contracts[50]

This directive covers abuses of power by the seller or supplier, in particular against one-sided standard contracts and the unfair exclusion of essential rights in contract".[51] It applies to the contracts that have not been individually negotiated by the parties, or that have been drafted in advance and the consumer has therefore not been able to influence the substance of the term" (see article 3).

In our view of an AmI environment, users are often confronted with non-negotiable one-sided general terms and conditions. In these general terms and conditions, the data protection rights of the user will be unilaterally defined by the profiler, while if the envisioned AmI world does come about, consumers will become increasingly dependent on AmI services.

The directive imposes mandatory rules of consumer protection: contracts should be drafted in plain, intelligible language; the consumer should be given an opportunity to examine all of the terms; and, if the terms are in doubt, the interpretation most favourable to the consumer should prevail (article 5).

Thinking on the concept of "ambient law" - a law that is effective without the subject being forced to actively agree every minute with contractual terms and conditions - one could imagine that consumer protection law, in particular this directive, could be the starting point for a new approach towards the protection of the user by obliging AmI service providers (using profiles) to draft contracts in a *technologically* intelligible language that gives the *intelligent agent* of the consumer an opportunity to examine all of the terms and to respond accordingly by refusing or allowing certain decisions, profiling practises etc.

7.1.3.4.B. Directive 97/7 on consumer protection in respect of distance contracts[52]

This directive covers consumer protection regarding distance contracts between suppliers and consumers.[53] The protection mainly consists of the determination of information required to be provided to the consumer. For example, prior to and in good time *before the conclusion of any distance contract*, the consumer must be provided in a clear and comprehensible manner with the identity of the supplier, with the main characteristics of goods and services; with the price of goods and services, including all taxes; with delivery costs etc. Because the information disseminated by certain electronic technologies is often *ephemeral* in nature insofar as it is not received on a permanent medium, consumers must also receive written notice in good time of the information necessary for proper performance of the contract.

---

[50] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *Official Journal L 095, 21/04/1993 P. 0029 - 0034.*

[51] *See preamble.*

[52] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *Official Journal L 144, 04/06/1997, P. 0019 - 0027.*

[53] Distance contracts are "contracts concerning goods or services concluded between a supplier and a consumer under an organised distance sales or service- provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded" (article 2.1.)

(article 5.1.). However, the mandatory written confirmation (in a durable, available and accessible medium) does not apply to 'services performed through the use of a means of distance communication, where they are supplied on only one occasion and are invoiced by the operator of the means of distance communication' (article 5.2.). Nevertheless, the consumer must always be able to obtain the geographical address of the supplier to which he may address any complaints.

If we again refer to the concept of ambient law we could image the provision of the required information and the negotiating of available options in a format that is intelligible for the intelligent agent of the consumer. The agent should incorporate the legislation in such a way that any proposed transaction that is in violation of the directive will be rejected automatically.

7.1.3.4.C. E-Commerce Directive 2000/31 [54]

This directive was adopted to ensure legal certainty, consumer confidence and free movement of 'information society services' between the EU Member States. The directive, as stated in recital 14, should be in full compliance with the principles relating to personal data protection, in particular as regards unsolicited commercial communication and liability of intermediaries.

The directive cannot prevent anonymous use of open networks such as the Internet. It contains important provisions regarding information to be provided and regarding liability. Section 4 of the Directive, titled "*liability of intermediary service providers",* constitutes a very important part of the directive.

- In the case of mere conduit[55], the service provider is not liable *for the information transmitted,* on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission (article 12.1.).
- In case of caching (article 13), service providers are not liable *for the automatic, intermediate and temporary storage of that information,* performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that the provider: (a) does not modify the information; (b) complies with conditions on access to the information (c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry (d) doesn't interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

---

[54] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *Official Journal L 178, 17/7/2000, P. 0001 - 0016.*

[55] Mere Conduit is "the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, including the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission" (article 12.1. & 12.2.)

- In the case of hosting (article 14), a service provider is not liable *for the information stored at the request of a recipient of the service*, on condition that (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

Regarding the liability of internet service providers, we underline that this directive does in fact not apply to legal issues concerning privacy and data protection. As a consequence, one can conclude that *notice-and-take down* procedures[56] may not be applicable in the case of infringements of privacy and data protection laws. We suggest that the notice-and-take down procedure could be a useful tool to provide control and safeguards in AmI environments.

Regarding the information obligation,[57] we refer again to the fact that this information should be given in a technologically intelligible form, understandable for the intelligent agent of the AmI user (ambient law).

7.1.3.5 Standards and interoperability

Standards and interoperability seem to be necessary for the creation of an AmI environment. They however do create vulnerability in terms of security and privacy.

From a legal point of view, an important distinction exists between the notions of 'technical regulations' and 'technical standards'. Technical regulations are created by authorised public authorities and are in principle binding. Most problems of interoperability are however not solved via technical regulations, but via technical standards.

Technical standards are prepared by all interested parties (companies, consumers, workers, public authorities) on the basis of a number of principles (e.g. consensus, openness and transparency)[58]. Although they can be very important to solve problems of interoperability, they are in principle not binding. To make these standards legally binding, they have to be included in legal acts.

---

[56] The "notice and take down" is a procedure that follows Article 14 of the E-Commerce Directive. This article states that hosting providers (providers that store information on a server) are not liable if they, after obtaining knowledge of illegal activity or information or becoming aware of facts and circumstances indicating illegal activity, act expeditiously to remove or to disable access to the "illegal" information. Actually, discussions are going on about when ISP's should initiate such a procedure because often, perfectly legal websites are taken down after notice by a private third party, without a court order, because ISP's want to avoid liability and claims for damage for the illegal content (the discussions are also about the concept of private censorship).

[57] Article 5, 6 and 10 of the E-Commerce Directive foresee, for example, that a recipient of an information society service must receive information from the provider regarding its name, physical and electronic address. In the case of commercial communications, the existence, content and origin of the commercial communication must be provided with. Prior to an order being placed, the recipient must be clearly informed of the technical steps and technical means, as well as of the languages offered for the conclusion of the contract.

[58] An extended overview of the European Commission's standardisation policy can be found in the "Vademecum on European standardisation" of the European Commission, available on http://europa.eu.int/comm/enterprise/standards_policy/vademecum/index.htm

Important legislation on EU level is Directive 98/34 on technical standards and technical regulations in information society services.[59] This directive imposes a detailed information procedure for technical standards and regulations: Member States are obliged to inform the Commission and other Member States of new initiatives in this field and to publish the draft standards in such a way that comments may also be obtained from parties established in other Member States (article 2-3). The Commission and other Member States will be allowed to propose amendments to a contemplated measure, in order to remove or reduce any barriers, which it might create, to the free movement of goods (article 6). The Member State concerned must take into account the amendments when formulating the definitive text of the measure envisaged. This procedure allows the Commission, the Member States and the economical operators to be aware of technical standards and regulations that the Member States want to install. The information and cooperation procedure foreseen in this directive can help the Commission in harmonising the standards and can eventually form the basis for the creation of European standards.

7.2 The second step: the construction of (group) profiles, including making personal data anonymous

The aim of constructing profiles by means of data mining techniques is to transform data into *knowledge*. This knowledge can in fact lead to the situation that the profile confronts people with information about themselves they did not know before.[60]

Two situations must be distinguished: the personal data used to construct profiles are rendered anonymous after their collection or they remain related to identified/identifiable persons.

- In the first situation, when data are rendered anonymous, data protection legislation may not apply. That would mean that people don not have access to the knowledge of the profiler and can not control the creation of group profiles that can concern them as a member of a group. Non applicability would have as a consequence that, for instance, article 12 of D95/46 EU, that reads that 'the data subject has the right to obtain from the controller (…) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15.1 does not apply'. This is not a desirable situation. When group profiles are applied - even if based on anonymous personal data - they can have major impact on people's autonomy and self-determination.
- In the second situation, if personal data are not rendered anonymous, data protection remains applicable. But the question remains whether and how the subject has the right to interfere in this process once the data controller has got the right to process the data for profiling purposes (see above). Control by the data subject exists mainly at the level of data collection. The right to object to processing of personal data for the purpose of direct marketing - although it is not clear what would constitute direct marketing in AmI - exists for example *de facto* only at the level of the data collection. We here refer to the discussions above. There are, however, some rights that can be invoked particularly at the level of the construction of profiles. They can contribute in

[59] Directive 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services, *Official Journal L 204, 21/07/1998 P. 0037 – 0048*.

[60] See Custers, B., "The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology", Nijmegen, Wolf Legal Publishers 2004.

an important manner to obtain knowledge of the profiles that incorporate one's personal data. One such important right can be found in the above- mentioned article 12. In practice, however, it may be difficult to invoke this right. The right to be informed whether or not personal data are being processed, the right to know the categories of data concerned and the right to obtain communication in an intelligible form of the data undergoing processing (article 12), is also of particular relevance in the stadium of profile construction because otherwise the data subject does not know which of the collected personal data concerning him, are finally used to construct the profile. Also the right to be informed who the recipients (or categories of recipients) of the data are (article 12), can be important because the transfer of the profile to third parties occurs often - mainly - after the construction of the database. But this right can only be invoked i*f necessary to guarantee a fair processing* (article 10), which again leaves the door open for discussion. As we have seen, the information of the *categories* of recipients is too broad and does not give clear indication by whom, where and when the profile will be used and applied. Finally, at this stage also, data subjects have the right to correct data and to object further processing when the controller anticipates personal data being processed for the purposes of direct marketing.

Lastly we should add that natural persons have in principle no (intellectual) property right to their personal data.[61] However, some authors do argue for an intellectual property right in "human identity".[62] Also Intellectual property rights to personal data may also exist in the case of profiles to the extent that they are in fact collections of personal data in the form of a database. In that case they may enjoy the sui generis intellectual right of the database,[63] when they are the result of a creation or a substantial investment of the maker of the profile. These creations and results are often trade secreted, patented or copyrighted. They are major assets of companies and are object of sharing, selling and licensing. In other words, when personal data are transformed into the correlated set of anonymous data that form a profile, they slip out of the control of the natural person and become property of a company.

7.3 *The third step: the application of (group) profiles*

7.3.1 The Data Protection Directive

Applicability of the directive at the application level generally depends on the identifiability of the person targeted - if application of a profile gives rise to some activity that falls within the scope of 'processing', as defined in article 2.b: 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection,

[61] See Samuelson, P., "Privacy as Intellectual Property?", *Stanford Law Review* 2000-52, p. 1125-1173.
[62] See Pinckaers, J.C.S., "7.3. Economic Reasons for an Intellectual Property Right in Human Identity" in idem, *From Privacy toward a New Intellectual Property Right in Persona*, Den Haag, Kluwer Law International, 1996, p. 245-257.
[63] This intellectual right is sui generis because it does not fit other categories of intelectual rights like patents, copyright etc. See Directive 96/9 EC on the legal protection of databases. However, see article 1.3 of the directive that reads: 'Protection under this Directive shall not apply to computer programs used in the making or operation of databases accessible by electronic means', and article 3.2 that spells out that: 'The copyright protection of databases provided for by this Directive shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves'.

recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'. Article 15, which concerns the automatic application of automated profiles to individuals, is very relevant in this second level. Also at this point, the distinction between group profiles and personalised profiles is relevant.

7.3.1.1 Group profiles

The application of group profiles in AmI environments implies that the group profile has to be activated in one way or another. This activation can occur in two ways, either the AmI environment detects personal data of identifiable persons that indicate the applicability of the profile, or the AmI environment detects data of non-identifiable persons or other information that indicate applicability. This distinction has consequences from a legal point of view. If personal data are detected (if the group profile applies to an identifiable person) data protection law applies: the rights of the subjects and the obligations of the data controller are defined (see infra). If the group profile is not applied to an identifiable person, data protection law does not apply.

7.3.1.2 Personalised profiles

If we start from the fact that the application of personalised profile requires the detection of personal data at the moment of application, data protection law applies in these situations. If the personalised profile is applied to a person using pseudonyms, data protection legislation may not apply if these pseudonyms can not be linked to an identifiable person[64]

7.3.1.3 Three examples before looking at article 15 of the directive

In the next paragraph we will discuss the applicability and application of article 15 of the directive to the application of profiles. We should stress, however, that especially in AmI, data collection, profile construction and application of the profile can take place at the same time.

7.3.1.3.A. Rock concert

This example shows that consent at the data collection level is difficult to refuse and that once data have been anonymised, control over the use of these anonymised data is lost.

An organiser of a rock concert sells tickets on-line and the subjects must give name, address, age and billing information. After issuing the ticket and receipt of payment, the personal data are made anonymous. The organiser uses the anonymous data to calculate the average age of the visitors. The outcome is that the 64 % of the visitors are under 18. Consequently, the price of '*breezers*' increases with 5 % because statistics have proven that 17- year- old children love these soft drinks…

In principle data protection law applies at the level of data collection: the data subject has to be informed of the purpose of profiling at the moment of collection if her personal data are used for the construction of the profile (see the discussion in section 7.1.3.2.A.3). The data

[64] This would mean that the pseudonym creates in fact total anonymity. If the pseudonym can be linked with an identifiable person (even if the identity behind the pseudonym is kept by a trusted third party), data protection law remains applicable.

subject could refuse that her data be used for such purpose, but then she may not get a ticket. However, as the construction of the profiles is based on data that are rendered anonymous, data protection law does not apply any more. Data protection will also not apply at the application level since the data subject is not identifiable at the moment of application.

7.3.1.3.B. Music in a restaurant

This example shows that anonymity as such does not prevent people from being determined.

In an AmI equipped restaurant, the style of music (jazz, rock, lounge, etc.) can change in function of the average preferences of the total amount of connected visitors. The visitor's preferences are processed through their anonymous communication devices and collected through a sensor network of the restaurant. Upon these data, an instant group profile is built. This group profile can be used for immediate adaptation of the music style, as well as for future music settings, based on the growing profile information.

Data protection law does not apply here at all. The anonymous communication infrastructure in the restaurant does not allow the restaurant to identify those present. Nevertheless, the restaurant knows the preferences of those present, while a computer calculates, plays, and changes the major music preferences of those present.

7.3.1.3.C. Interactive television at home

This example shows the many actors involved in data collection and profile application, and the difficulties to obtain transparency and control over the use of your own personal data. It also demonstrates the fragmentation of our society, or the loss of a “common reality”, as everybody will receive different information and will enter into his own reality.

To provide the best home entertainment experience, interactive television providers monitor and store *exactly* what is being watched on each television. Using these data, computers are capable of calculating *perfectly* what kind of content has been watched by the largest group of televisions (group profile) and what content has been watched on a particular television (personalised profile). By the examination of the group profile, broadcasters can stop buying or producing programs that are not often viewed. These group profiles can be sold to other television broadcasters. The computer will also be capable to anticipate which content will be broadcasted in the future and for what price, and this towards each individual television. The broadcaster can also, for instance, use customer databases of supermarkets. By linking the IP-addresses of televisions to the physical addresses of supermarket customers (obtained for the purpose of delivery of goods), supermarkets could buy exclusivity to provide commercial messages towards particular televisions, or to provide exclusive e-commerce applications in the food- sector towards particular televisions.

Watching behaviour is a type of personal data, as far as it is related to an identifiable person. This would mean that in principle the data subject must be informed about the purposes of the data collection, like the building and application of profiles (see section 7.1.3.2.A.3). Data protection is not applicable for the construction of the group profile, if this is built upon anonymised data, while it is applicable for the construction of a personalised profile if this can be related to an identifiable person. In the latter case, the recipients or the categories of recipients of the personalised profiles must be communicated to the data subject. As we have seen, such communication of rather abstract categories of recipients does not really help the

data subject to control his/her own data. If supermarkets provide the personal data to third parties, the data subject has to be notified of this possible transfer.

7.3.1.4 Automated decisions in group profiling and personal profiling

Special attention should be paid at article 15 of the directive. This article deals with so-called "*automated individual decisions*" and it strongly related to profiling. [65]

Article 15(1) states: "*every person has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.*"

However, article 15 (2) contains again exceptions and states that "*a person may nevertheless be subjected to an automated individual decision if that decision is taken [a] in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view, or [b] is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests*".

Contrary to the other provisions of the data protection directive, this article may be read regardless of the question whether or not the application of the profile involves collecting data of an identifiable individual or not. In fact, according to the Commission, article 15 has been designed to protect the interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'.[66] The Commission also stated that "the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities".[67]

We did not find case law regarding this article. Lee Bygrave analysed the possible impact of this article on automated profiling in "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling".[68] According to Bygrave, article 15(1) does not directly *prohibit* a particular type of decision-making or profile application. Rather it confers on persons a right to prevent them being subjected to such decision making, if their

---

[65] The original proposal for the Privacy and Electronic Communications Directive 2002/58 also contained a specific provision on profiling, stating that "the telecommunications organization shall not use personal data on subscribers to set up electronic profiles of the subscribers or classifications of individual subscribers by category" (See Article 4(2) of the Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the Integrated Services Digital Network (ISDN) and public digital mobile networks (COM(90) 314 final - SYN 288, 13.9.1990). The provision was deleted from later drafts "in order to take account of the principle of subsidiarity" (See COM(94) 128 final - COD 288, 13.6.1994, p. 8).

[66] COM(90) 314 final - SYN 287, 13.09.1990, 29.

[67] COM(92) 422 final - SYN 287, 15.10.1992, 26.

[68] Bygrave, Lee A., "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law & Security Report*, 2001, volume 17, pp. 17–24; *Privacy Law & Policy Reporter*, 2000, volume 7, pp. 67–76

personal data are processed. This would "leave the actual exercise of the right to the discretion of each person and allow, in effect, the targeted decision making to occur in the absence of the right being exercised". In other words, Bygrave suggests that the data subject involved must actively exercise his right not to be subjected to automated decision making *if his personal data are processed*. It is not clear whether a person has the right to *a posteriori* nullify a decision, for example, in the case of automated decisions that are taken without his prior consent. Article 15 does not seem to impose the condition of prior consent of the data subject to be subjected to automated decision making.

However, article 15 does not *prevent* national legislators from implementing it in terms of an explicit prohibition on *targeted decision making*. The Belgian Data Protection Act of 1992, revised in 1998, contains indeed in article 12b is an explicit prohibition that goes further than the minimum requirements of the Directive: "*A decision resulting into legal effects for a person or affecting him seriously, may not be taken purely on the basis of automatic data processing that is destined for the evaluation of certain aspects of his personality. The prohibition laid down in the first section is not applicable if the decision is taken in the context of an agreement or if it has its ground in a provision laid down by or by virtue of a law, decree or ordinance. In such agreement or provision appropriate measures shall be taken for the protection of the legitimate interests of the data subject. At least he shall be allowed to bring up his standpoint in a useful way.*"[69]

Furthermore, Bygrave analyses the difficulties that exist in interpreting the provisions laid down in article 15. It is not easy to anticipate what should fall within the cumulative conditions of the article: do personalised advertising banners, that automatically adjust their content according to the visitor's profile, involve an automated decision that significantly affects data subjects; when do decisions produce legal effects; when do decisions "significantly affect" data subjects; in which case can a decision be said to be based solely on automated data processing?

7.3.2 Privacy and Electronic Communications Directive 2002/58

The Directive (article 13) contains a special provision concerning *unsolicited communications towards natural persons*. It puts an end to the long lasting controversy regarding direct marketing, by explicitly adopting an opt-in system that inherently implies the prohibition of unsolicited marketing mail or communications.[70] The use of e-communication media such as e-mail and SMS for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent for it (*opt-in*), except where the electronic contacts were obtained directly from the customer in the context of a sale of a product or service for similar products and services, provided that the customer has a clear and easy opportunity to object to such use at the moment of collection and on the occasion of each message (*opt-out*).

What direct marketing is has not been defined in the directive. Article 13 only states that unsolicited communication has to relate to direct marketing: "The use of automated calling systems without human intervention (automatic calling machines), facsimile machines fax) or

[69] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals laatst gewijzigd door de wet van 11 december 1998, *B.S.* 3 februari 1999.

[70] See EPIC&Privacy International, *Privacy and human rights 2002. An international survey of privacy laws and developments*, Washington/London, 2002, p. 12., http://www.privacyinternational.org/survey/phr2002.

electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent."[71]

It is clear, however, that the communications need to have a commercial content in order to fall under the opt-in regulation of directive 2002/58. Considerans 40 indicates that direct marketing relates to commercial communications only: "Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. *These forms of unsolicited commercial communications* …"

As seen before, it is not clear whether personalised *experiences* in AmI environments and/or the *delivery* of AmI personalised goods and services, can be considered as direct marketing. In the case of AmI experiences and delivery of goods and services, there is no "marketing" because the goods and services are in fact often supplied without being preliminary promoted.

7.3.2.1 E-commerce and Consumer Protection Law; Standards and Operability

We refer to sections 7.1.3.4 and 7.1.3.5.

[71] EU directive 2000/31 on Electronic Commerce defines "commercial communication" as "any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession". The following do not in themselves constitute commercial communications: - information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address; - communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration;

8 Conclusions

This document presents a preliminary exercise on AmI and profiling. It draws on the existing work done on profiling in FIDIS deliverable 7.2 and adds a first exploration of AmI in the form of simple examples and tentative definitions. The aim of the document is to provide insight into the conditional relationship between profiling and AmI rather than to provide an extensive overview of the field of AmI.

The main issues to be solved for a successfully networked and adaptive environment have been located in the domains of interoperability, privacy and security. Interoperability may seem to warrant technical solutions first, but – as explained in FIDIS deliverable 4.1 – without effective communication and trust these technical solutions will not be conclusive. Solutions to issues of privacy and security have been explored from the perspective of enhancing user control. As chapters 6 and 7 of this deliverable clearly indicate, such solutions need integration of technological and legal tools. Legislation that is technically, socially and/or economically not feasible will not amount to any substantial protection, while privacy enhancing technologies that promote user control may not catch on if the law does not effectively constrain the production and usage of privacy invading design.

9 Abbreviations and Glossary

BAN: Body Area Network

CC/PP: Composite Capabilities / Preferences Profile

DRM: Digital Rights Management

IMD: Identity Management Device

ISDN: Integrated Services Digital Network

LAN: Local Area Network

PAN: Personal Area Network

PII: Personally Identifiable Information

PSTN: Public Switched Telephone Network

RFID: Radio Frequency Identity Tags

RDF: Resource Description Framework

UAProf: User Agent Profile

WAN: Wide Area Network

WAP: Wireless Access Protocol

ambient law legal regulation integrated with computer code (for instance on the PDA of a data subject), that regulates the subjects interactions with an AmI environment in accordance with data protection and/or other relevant legal norms

see chapter 7.1.3.2.B.1, 7.1.3.4.A, 7.1.3.4.B of this deliverable

data controller: the subject (a natural or legal person) that determines alone or jointly with others the purposes and means of the processing of data

see also Directive 95/46 EU on Data Protection, concerning processing of personal data, article 2 sub d

data mining: data processing using sophisticated data search capabilities and statistical algorithms to discover patterns and correlations in large pre-existing databases; a way to discover new meaning in data

see http://www.elook.org/dictionary/data-mining.html

data subject: the subject (human or nonhuman), individual or group that data refer to

data processing:

computer science: a series of operations on data by a computer in order to retrieve or transform or classify information

see http://www.elook.org/dictionary/data-processing.html

legal: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

Directive 95/46 EU on Data Protection, concerning processing of personal data, article 2 sub b

phishing the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft

see: http://www.webopedia.com/TERM/p/phishing.html

personal data:

(*common sense*): any data that refer to a person, whether or not identified or identifiable

legal: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

Directive 95/46 EU on Data Protection, article 2, sub a

profile: set of correlated data that identifies and represents a data subject. If the data subject is a group/a category/or a cluster we speak of a group profiles, when the data subject is a single person we speak of a personalised profile.

See FIDIS deliverable 7.2, chapter 2

profiling: the process of constructing profiles (correlated data), that identify and represent a data subject (either a person or a group/a category/a cluster), and/or the application of profiles (correlated data) to identify and represent a person as a specific person or as member of a specific

group/category/cluster, aiming at the assessment of risks and/or opportunities for the data user (inferred from risks and opportunities concerning the data subject)

See FIDIS deliverable 7.2, chapter 2

(end) user: the data subject that uses a service and/or a device (personal digital agent, web, customer loyalty card), whose data are recorded and processed and/or to whom a profile is applied

10 Bibliography

Aarts, Emile and Marzano Stefano 2003, "*The New Everyday. Views on Ambient Intelligence*", Rotterdam: 010.

Alexandra Institute's Centre for IT Security in collaboration with Peter Blume from University of Copenhagen, "*Pervasive computing - IT security and privacy*", Report prepared for the Danish Council for IT Security, available at http://www.rfits.dk/English.3349.0.html

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F. and Rohs, M. 2004, "Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing", Institute for Pervasive Computing, ETH Zurich, Switzerland, available at: www.vs.inf.ethz.ch/publ/papers/socialambient.pdf

Bygrave, Lee A. **2000**, "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law & Security Report*, 2001, volume 17, p. 17-24; *Privacy Law & Policy Reporter*, 2000, volume 7, p. 67–76

Clements, B., Maghiros, I., Beslay, L., Centeno, C., Punie Y. & Rodriguez 2003, C. *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS-JRC, July 2003, available at http://www.jrc.es/home/pages/detail.cfm?prs=1118

Coen, M. H. 1998, "Design principles for intelligent environments," in *Proc. 15 Nat./10th Conf. Artif. Intell./Innovative Applicat. Artif. Intell*. Madison, WI, p. 547-554.

Custers, B. **2004**, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Nijmegen, Wolf Legal Publishers

Delaitre, S. 2005, "Identity: facets and vulnerabilities in ambient intelligence environment", *EICAR Best Paper Proceedings 2005 conference*. ISBN:87-987271-7-6, pp 154-166

Dertouzos, M. L. 1999, "The future of computing", *Scientific American* (281), 2, p. 52-55

Dinka D. and Ingmarsson M. 2003? A*mbient intelligent at home*, White paper in the EU-founded project Ambient Intelligence To Go: AmIGo, available at: http://www.santaanna.se/projects.html

EPIC & Privacy International 2002, *Privacy and human rights 2002. An international survey of privacy laws and developments*, Washington/London, p. 12, available at: http://www.privacyinternational.org/survey/phr2002.

Irwin, Alan 2001, "Citizen engagement in science and technology policy: a commentary on recent UK experience", *PLA Notes* 40

ISTAG 2001 (Information Society Technology Advisory Group), *Scenarios for ambient intelligence in 2010*, available at: http://www.cordis.lu/ist/istag-reports.htm

ISTAG 2002, *Software technologies, embedded systems and distributed systems*, available at: http://www.cordis.lu/ist/istag-reports.htm

ISTAG 2003, *Ambient Intelligence: From vision to reality. For participation - in business & society*, available at: http://www.cordis.lu/ist/istag-reports.htm

ISTAG 2004, *GRIDS, Distributed Systems and Software Architectures*, available at: http://www.cordis.lu/ist/istag-reports.htm

Lessig, L. 1999, *Code and OtherLaws of Cyberspace*, New York, Basic Books

Menduiña E. 2005, *Integration of biometrics in Smart Homes*, 2nd BioSec Workshop, Brussels, January 2005, available at http://www.biosec.org/index.php

NEC corporation 2003, *Mobile Digital Rights Management White Paper* 2003, available at: http://www.nec-mobilesolutions.com/application/products/drm.html.

Nicoll, C., Prins, C., van Dellen, M.J.M. (Eds) 2003, "*Digital Anonimity and the Law. Tensions and Dimensions*", The Hague, TMC Asser Press

O'Hare, G.M.P., O'Grady, M.J., Keegan, S., O'Kane, D., Tynan, R. & Marsh, D. 2004 *"Intelligent Agile Agents: Active Enablers for Ambient Intelligence,"* AISD, SIGCHI workshop, Vienna

Pinckaers, J.C.S. 1996, "7.3. Economic Reasons for an Intellectual Property Right in Human Identity" in idem, *From Privacy toward a New Intellectual Property Right in Persona*, The Hague, Kluwer Law International, p. 245-257

Plomb, J. and Tealdi, P. 2004, *Ambient Intelligent Technologies for Wellbeing at Home–* EUSAI 2004, Eindhoven, The Netherlands, available at http://www.eusai.net/

Raisinghani, Mahesh S., Benoit, A., Ding, J. , Gomez, M., Gupta, K., Gusila, V., Power, D. and Schmedding, O. 2004, "Ambient Intelligence: Changing Forms of Human-Computer Interaction and their Social Implications", *Journal of Digital Information*, 2004 (5)

Ranse, Stéphanie 2004, "Le profiling des internautes au regards du droit au respect de a vie privée: le coût de l'efficacité !", *Revue du Droit des Technologies de l'Information*, 2004-20, p. 37-58

Reidenberg, J. 1998, "Lex Informatica: The Formulation of Information Policy Rules Through Technology", 76 *Texas Law Review* 553

Remagnino, P. and Foresti, G.L. 2005, "Ambient Intelligence: A New Multidisciplinary Paradigm", *IEEE Transactions on Systems, Man and Cybernetics*, Part A: Systems and Humans, (35), 1, p. 1-6.

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 2003, available at

http://www.vepsy.com/communication/book4/4_04RIVA.PDF

Riva, G., Vatalaro, F., Davide, F., Alcaniz, M. (eds.) 2005, *Ambient Intelligence: The Evolution Of Technology, Communication And Cognition Towards The Future Of Human-Computer Interactio*", IOS Press 2005, available at: www.ambientintelligence.org, and http://www.vepsy.com/communication/volume6.html

Samuelson, P. **2000**, "Privacy as Intellectual Property?", *Stanford Law Review* 52, p. 1125-1173

Schaefer, R., Eikerling, H.-J. 2004, *Increasing the Acceptance of Ambient Intelligent Technologies for Wellbeing at Home through Security Contexts – EUSAI 2004*, Eindhoven, The Netherlands, available at http://www.eusai.net/

Schuurmans, J., Zijlstra, E. 2004, *Towards a continuous personalization experience*, http://www.sigchi.nl/papers/2004-Schuurmans-EtAl.pdf.

Van Loenen (2003), E., "On the role of Graspable Objects in the Ambient Intelligence Paradigm", *Proceedings of the Smart Objects Conference*, May 15-17 2003, Grenoble, France http://www.grenoble-soc.com/proceedings03/Pdf/Van%20Loenen.pdf,

Wagelaar, D., Georges, A., Rigole, P., Clerckx, T., Berbers, Y., Coninx, K., Jonckers, V., De Bosshere, K., Preuveneers, D., and Van den Bergh, J. 2005, "Toward an extensible context ontology for ambient intelligence" *Proceedings 2nd European Symposium Ambient Intelligence*, Eindhoven, The Netherlands, Nov. 8-10, 2004, to be published

Weiser, M. 1991, "The Computer for the 21st Century", *Scientific American*, (265) 1991-3, p. 94-104.

Zarsky, T. 2002, "Cookie Viewers and the Undermining of Data-Mining: A Critical Review of the DoubleClick Settlement", *Stanford Technology law Review*, http://stlr.stanford.edu/STLR/Events

Zheng Yan 2002, *Mobile Digital Rights Management*, T-110.501 Seminar on Network Security 2001, Publications in Telecommunications Software and Multimedia TML-C7, Espoo, 2002, available at http://www.tml.tkk.fi/Studies/T-110.501/2001/papers/

Relevant Internet Portals:

www.cordis.lu/ist/istag.htm

EU Information Society Technology Advisory Group

http://swami.jrc.es

SWAMI (**Safeguards in a World of Ambient Integlligence**), an IST Sixth Framework Programme funded project, aims to identify and analyse the social, economic, legal, technological and ethical issues related to identity, privacy and security in the forecasted but not yet deployed Ambient Intelligence (AmI) environment.

www.ist-eperspace.org

The main objective of the ePerSpace project (**Towards the Era of Personal Services at Home and Everywhere**), an IST Sixth Framework Programme funded project, is to significantly increase the user acceptance of networked audiovisual systems and applications at home and virtually anywhere by developing innovative interoperable value-added networked services. From an industrial perspective, ePerSpace aims at creating a mass-market adoption of such advanced services thanks to this significantly increased user acceptance.

http://www.mosaic-network.org

MOSAIC (**Mobile Worker Support Environments**), an IST Sixth Framework Programme funded project, develops scenarios and roadmaps for mobile and location-aware working,

builds strategies for deploying innovative mobile work technologies and applications in sector domains, and starts up initiatives for joint research and innovation.

http://odin.agr.unideb.hu/magisz/Projektek/AMI-Netfood/Public/AMI-Netfood.htm

The objective of AMI@netfood project (**Development of Long-term shared vision on AMI Technologies for a Networked Agri-food sector**), an IST Sixth Framework Programme funded project, is to support the implementation of the IST Research Priority and Framework Programme, providing a long-term vision on future trends on Scientific and Technology Research oriented to the development and application of Ambient Intelligence technologies to agri-food domain.

http://www.ask-it.org/

Ambient Intelligence System of Agents for Knowledge-based and Integrated Services for Mobility Impaired users (ASK-IT) (an IST Sixth Framework Programme funded project) aims at establish Ambient Intelligence (AmI) in semantic web enabled services, to support and promote the mobility of Mobility Impaired people, enabling the provision of personalised, self-configurable, intuitive and context-related applications and services and facilitating knowledge and content organisation and processing.

http://www.bmtproject.net/mapped/index.html

Mobilisation and Accessibility Planning for PEople with Disabilities (MAPPED), (an IST project partially funded project by the Sixth Framework Programme), will provide users with the ability to plan excursions from any point to any other point, at any time, using public transport, their own vehicle, walking, or using a wheelchair, taking into consideration all their accessibility needs.

www.ambientintelligence.org

Website on AmI, e-health, virtual reality and future technologies and health-care

http://ami.inigraphics.net

Several departments of the INI-GraphicsNet **(the International Network of Institutions for advanced education, training and R & D in Computer Graphics technology, systems and applications**) bunch their research experiences and efforts to make the vision of Ambient Intelligence become true.

http://www.eusai.net/

Site of the Second European Symposium on Ambient Intelligence (euSAI), November 8th-10th 2004, Eindhoven, the Netherlands

http://www.soc-eusai2005.org/index.php

Site of the Joint sOc (smart Objects conference) & euSAI (european Symposium on Ambient Intelligence) on **Smart Objects & Ambient Intelligence,** October 12th - 14th 2005, Grenoble, France