FIDIS

Future of Identity in the Information Society

| | |
|---|---|
| Title: | "D7.9: A Vision of Ambient Law" |
| Author: | WP7 |
| Editors: | Mireille Hildebrandt (VUB), Bert-Jaap Koops (TILT) |
| Reviewers: | Claudia Diaz (COSIC)<br>Jozef Vyskoc (VaF) |
| Identifier: | D7.9 |
| Type: | [Report] |
| Version: | 1.0 |
| Date: | Thursday, 04 October 2007 |
| Status: | [Final] |
| Class: | [Public] |
| File: | fidis-wp7-d7.9_A_Vision_of_Ambient_Law |

## *Summary*

This report addresses the research question: can law as embodied in the future Ambient Intelligence architecture – Ambient Law – safeguard the core values of privacy and non-discrimination, while at the same time helping to realise the potential of Ambient Intelligence? This question is answered by analysing Ambient Intelligence and the role of Ambient Law therein from a conceptual, legal, and technical perspective.

*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** | 06.05.2007 | • Initial release (Mireille Hildebrandt) |
| **0.2** | 05.06.2007 | • Revised structure; outline inserted; minor edits (BJK, MH) |
| **0.3** | 29.06.2007 | • inserted PET-TET and digital territories contributions and revised scenario 2; minor edits (MH, BJK) |
| **0.4** | 24.07.2007 | • inserted introduction, legal chapter and revisions of technical chapter and scenario 1; major edits and comments (BJK)<br>• revision of chapter 3, first draft of chapter 6, minor edits (MH) |
| **0.5** | 15.08.2007 | • inserted revised chapters 4-6; various edits; Executive Summary (BJK; MH)<br>• final version for internal review |
| **0.6** | 17.09.2007 | • integration of comments of the reviewers, new version sent to the authors with request to amend |
| **1.0** | 02.10.2007 | • final version |

# Foreword

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

| *Chapter* | *Contributor(s)* |
|---|---|
| **Executive Summary** | Bert-Jaap Koops (TILT) |
| **1 Introduction** | Bert-Jaap Koops (TILT), Mireille Hildebrandt (VUB) |
| **2 Two AmI scenarios** | Vassiliki Andronikou (ICCS), Mark Gasson (Reading) |
| **3 A Vision of Ambient Law. Conceptual Exploration** | Mireille Hildebrandt (VUB) (with Barbara Daskala (IPTS) for §3.5.3) |
| **4 Assessment of the Existing Legal Framework** | Sven van Damme, Eleni Kosta (ICRI) |
| **5 Assessment of PETs and TETs** | Martin Meints, Marit Hansen (ICPP), Ammar Alkassar (Sirrix) |
| **6 How to Achieve Ambient Law** | Mireille Hildebrandt (VUB), Bert-Jaap Koops (TILT) |
| **7 Conclusion** | Mireille Hildebrandt (VUB), Bert-Jaap Koops (TILT) |
| **8 Third scenario** | Mireille Hildebrandt (VUB) |

# Table of Contents

# Abbreviations

| | |
|---|---|
| DRM | Digital Rights Management |
| DT | D1gital Territ0ries |
| ECHR | European Convention of Human Rights and Fundamental Freedoms |
| EU | European Union |
| HMI | human machine interface |
| IMS | identity-management system |
| IPTS | Institute for Prospective Technological Studies |
| M2M | machine-to-machine |
| OJ | Official Journal |
| P3P | Platform for Privacy Preferences |
| PET | Privacy-Enhancing Technology |
| PII | personally identifiable information |
| PPDM | Privacy Preserving Data Mining |
| TC | Trusted Computing |
| TET | Transparency-Enhancing Technology |
| TTP | Trusted Third Party |
| VLE | Virtual Learning Environment |
| VR | Virtual Residence |
| XML | eXtensible Markup Language |
| XPref | a preference language for P3P |

# Executive Summary

Ambient Intelligence is a development of ICT which seamlessly integrates smart devices with a smart environment. If the vision of Ambient Intelligence (AmI) comes true, we move to an age where we equip our entire environment with tools to 'think' of its own and to make 'smart' decisions for us. No doubt AmI will emerge somehow somewhere in the future, but *how* it will look like is yet an open issue. Widely diverging scenarios are possible, with a very different look and feel for its users.

This report focuses on an essential element of how AmI will turn out: can it incorporate core values of the democratic constitutional state, in particular privacy and non-discrimination? Rather than approaching this question by describing a bleak, Big Brother vision of AmI, this reports uses a more constructive and forward-looking perspective, by bringing our conception of law a step forward. We use the concept of Ambient Law (AmL) as a key direction of thought for developing Ambient Intelligence. This denotes an integration of legal norms and the technologies these norms aim to regulate. It builds on concepts like 'code as law' (Lessig) and 'value-embedded design' (Nissenbaum), but it is new in that it claims that the norms embodied in technology should be constituted as *legal* norms.

This leads to the **research question** of this report: can law as embodied in the future Ambient Intelligence architecture – Ambient Law – safeguard the core values of privacy and non-discrimination, while at the same time helping to realise the potential of Ambient Intelligence? This question is answered by analysing Ambient Intelligence and the role of Ambient Law therein from a conceptual, legal, and technical perspective.

Conceptually, modern law depends on the printed script – 'law in the books', and hence, the formulation and the enforcement of the rule are often separated. Ambient Law differs from this, in that it could embed legal rules in the technological and organisational architecture of AmI in a way that ensures enforcement, supposedly in an uncircumventable way, e.g., a smart car that cannot start if it detects a drunk driver. ICT-embedded law does not have to replace text-based, printed law but – on the contrary – in an AmI world, 'law in the books' can be complemented with 'law in other technologies' to improve legal protection in an AmI world.

The legal analysis shows that core principles of the data-protection framework, notably data minimisation, purpose specification, goal binding, informed explicit consent, and accountability, are entirely at odds with the vision of Ambient Intelligence. AmI cannot develop at all if the current legal framework is applied. The development of new emerging technologies and AmI applications and systems should not be hindered from the start by legal provisions based on an increasingly outdated paradigm of preventing data processing. The vision of AmI therefore requires a revision of the legal data-protection framework as it currently exists, perhaps along the lines of 'contextual integrity' (Nissenbaum).

At the same time, the core values *behind* privacy and data protection, such as autonomy, self-development, and human dignity, also imply that AmI should not be allowed to develop in a legal vacuum. Where current guiding principles of the legal framework increasingly fall short, other mechanisms must be established to maintain some form of balance between users (consumers, citizens) and providers (businesses, government). Moreover, also autonomy and non-discrimination are at risk when AmI applications seamlessly and invisibly make customised decisions about people. A first prerequisite for non-discrimination in an AmI world is transparency, which is unlikely to be affected by mere legislative or self-regulatory measures of AmI providers. One problem with self-regulatory measures is that providers have

a lot to gain from learning as much as possible about their users and much less incentives to protect their users' privacy.

It is here that the technological perspective can help. Privacy-Enhancing Technologies (PETs) and Transparency-Enhancing Technologies (TETs) have a great potential of filling the gaps in legal protection that AmI creates. To enhance transparency, purpose-specification, and informed consent, tools like P3P and History Management have been developed, while DRM and Trusted Computing could add alternative ways to track personal data and the way they are being processed. Such tools should be embedded in a personal device, like a PDA, which enables users to automatically interact with the AmI environment, while keeping substantial control over data flows and while identifying the AmI provider (perhaps in a reversibly pseudonymous way) who processes data and profiles them. The PET- and TET-based PDA enables users to monitor the intelligent environment's anticipating actions (which are based on profiles), so that they can decide whether they want to comply, change their behaviour, or complain because the profiling is based on unjust criteria. AmI users should not have to make such decisions all of the time, of course: their PDA should learn in which cases they go along with the environment and in which cases they want to be informed of profiling in order to make a case-specific decision, and it should translate the environment's profiling in such a way that the user understands what happened.

However, this technological perspective is largely theoretical today. Many PET concepts and tools exist, but they are not broadly used in practice. Moreover, today's PETs focus on personal data but are not developed to deal with group profiling, and most PETs work in the world of telecommunications but not in a comprehensive AmI setting comprising of all areas of users' lives. There is much work to do, then, if PETs are to fulfil their promise of protecting users in an AmI environment. This is all the more true for TETs, which have been much less researched than PETs and for which only some components are available.

The **conclusion** that can be drawn from the conceptual, legal, and technical analysis, is that AmL can in fact significantly help to safeguard the core values of privacy and non-discrimination, without obstructing the development of Ambient Intelligence as such. It acts as a check on AmI providers who may know too much of AmI users or make unjustified decisions about them. To a much further extent than the present legal framework, the integration of legal rights of opacity and transparency with the technological architecture would enable citizens to actually exercise these rights. Building in these core values into the AmI architecture will help to enhance its social and legal acceptability and will thus further the development of AmI.

This will not be easy, however. It cannot be taken for granted that the embedded rules have sufficient legitimacy. Making technology-embedded rules meet core principles of law is a daunting task indeed. However, this should not deter us from trying. Otherwise, bleak alternatives arise, illustrated in this report by two scenarios: a provider-centric scenario where users are manipulated by 'the system' without knowledge or redress, and a user-centric scenario where AmI does not fulfil its potential since the environment is rather stupid and quite user-unfriendly. Therefore, we conclude that the vision of Ambient Law should be used as an important roadmap for making the vision of Ambient Intelligence come true, in such a way that the core values of privacy and non-discrimination are safeguarded.

Much is needed to further develop, refine, and implement this vision. We **recommend** that at least the following issues are taken up for further research:

1. revising the legal framework of privacy and non-discrimination in light of the advent of Ambient Intelligence;
2. creating an adequate legal framework for generating and applying profiles;
3. developing PET- and TET-based human machine interfaces that allow individual citizens to communicate with their environment;
4. developing technological tools and redefining legal rules in such a way that the rules can be digitised and built-in in the AmI architecture;
5. developing mechanisms for ensuring the legitimacy and conformity with core legal principles of technology-embedded rules.

# 1 Introduction

## 1.1 Background: the vision of Ambient Intelligence

Ambient Intelligence is a development of ICT which seamlessly integrates smart devices into the environment. The home, the workplace, the shopping-mall – all kinds of private, semi-public, and public spaces will become equipped with embedded technologies that interact with the people moving in them. This development is known under various labels, such as Ubiquitous Computing. In this report, we use the term Ambient Intelligence (AmI),[1] which has a rich association potential. It stresses a fundamental change in the way mankind will interact with its surroundings. While man has through the ages slowly developed intelligence, lately also embedding this in sophisticated devices, we now move to an age where we equip our entire environment with tools to 'think' of its own and to make 'smart' decisions for us.

In an AmI world, people will be surrounded by intelligent interfaces supported by computing and networking technology that is everywhere and embedded in everyday objects like walls, screens, furniture, clothes, vehicles, and roads. In the vision of Ambient Intelligence, computing capabilities are always on, connected, present everywhere, enabling people and devices to interact with each other and with their environment.[2] The enabling technologies of AmI, such as RFID and other sensor technologies, data mining, and above all profiling – as described in earlier reports[3] –, are quickly moving forward. Nevertheless, AmI is still a vision, and it will take considerable time for it to become a reality. We do not doubt *that* AmI will emerge in some form or another at some point in time. It is rather *how* exactly AmI will look like that is the important question. Widely diverging scenarios are possible, depending on how, for what purposes, and by whom the AmI architecture will be determined. And these diverging scenarios have a very different look and feel for the users who will have to live in these future environments.[4] The scope and adequacy of legal protection is one element of this AmI look and feel, and this brings us to the topic of this report: the role of the law in determining the architecture of Ambient Intelligence.

## 1.2 Aim and research question: towards Ambient Law

What particularly interests us here is how an AmI world can incorporate core values that are key to the democratic constitutional state.[5] In particular, it is questionable whether privacy and data protection, as well as non-discrimination, can be safeguarded in an AmI environment by the legal instruments that we know today. Rather than approaching this question by describing a bleak vision of AmI that despairs over the presumed demise of traditional legal principles – which is quite likely to lead to backward-looking conclusions to curb the development of AmI, we want to start from a different, more forward-looking perspective.

Let us simply suppose that Ambient Intelligence is a highly attractive vision of the future. It has an enormous potential to making our lives easier and more comfortable, and so, let us assume that the development of AmI should be cherished and stimulated. What, then, is the

[1] As introduced by the Information Society Technology Advisory Group, see ISTAG 2001 and ISTAG 2003.

[2] Yves Punie, 'A social and technological view of Ambient Intelligence in Everyday Life: What bends the Trend?', Key Deliverable, The European Media and Technology in Everyday Life Network, 2000-2003, p. 8

[3] See FIDIS deliverables D7.3 and D7.7, available at http://www.fidis.net/fidis-del/, and SWAMI deliverables D1 and D4, available at http://swami.jrc.es/.

[4] Cf. the dark scenarios developed in SWAMI, D2, available at http://swami.jrc.es/pages/dark_scenarios.htm.

[5] Cf. FIDIS deliverable D7.4, available at http://www.fidis.net/fidis-del/.

role of the law in developing the AmI architecture? Our **aim** in this report is to study how core constitutional values like privacy and non-discrimination can be safeguarded, while at the same time the development of AmI is fostered.

For such a combination of potentially clashing interests to be possible, we think that our conception of law should be brought a step forward. Law in its current embodiment – let us for simplicity's sake call it 'law in the books' – is likely to fail in the face of AmI; it is highly doubtful that legal texts can be enforced in a world where the environment makes continuous, real-time, and autonomic decisions about the people moving in it. We use the concept of Ambient Law – a concept developed by Mireille Hildebrandt (2008) – as a key direction of thought for developing Ambient Intelligence. Ambient Law (AmL) denotes an integration of legal norms and the technologies these norms aim to regulate. Rather than relying on law in the books, the AmI world will need to rely on law embodied in technology itself.

Ambient Law thus builds on concepts like 'code as law' (Lessig) and 'value-embedded design' (Nissenbaum), but it is new in that it claims that the norms embodied in technology should be constituted as legal norms. This implies, among other things, that their enactment should entail sufficient democratic legitimation, while their application must be contestable in a court of law.[6] The **research question** that is central to this report can be formulated as follows:

> can law as embodied in the future Ambient Intelligence architecture – Ambient Law – safeguard the core values of privacy and non-discrimination, while at the same time helping to realise the potential of Ambient Intelligence?

## 1.3 Scenarios

Since this deliverable is future-oriented, we thought it useful to illustrate the developments we are sketching here in various scenarios. These scenarios are not expectations or predictions of the future, but stories that illustrate possible developments of the world in a timeframe of a few decades. These stories may help readers in visualising and realising the kinds of world that Ambient Intelligence may create for us. Put differently, the stories may also help policy makers and technology developers to envision what kinds of world they are creating in the middle or longer term when working on Ambient Intelligence. At this point in time, fundamental choices can – and in our opinion should – be made with respect to the architecture of AmI. One such fundamental choice is the architecture of control: who will be able to push the buttons of AmI environments? The importance of this choice is well illustrated by offering two extreme scenarios: one with AmI providers in total control, and one with users at the buttons.

The scenarios have been developed during a Workshop in January 2007 and further discussed among the authors via email. To explain how the scenarios came into being, we shall now briefly go into Shoemaker's steps for developing scenarios, taking into account that we use the scenarios here as a heuristic, not as an actual planning tool, for illustrative purposes (Shoemaker 1995).

1. **Define the scope (time frame)**

[6] Cf. on the democratic and constitutional acceptability of technologically embodied norms, Dommering and Asscher 2006, and Koops 2007.

The vision of Ambient Law concerns the vision of Ambient Intelligence, so the time frame is 5-25 years.

**2. Identify the major stakeholders (who will be affected, who could influence)**

The major stakeholders are citizens, businesses, and government authorities.

a. Citizens can influence the development of AmI by rejecting the technologies, by buying them or by using them in ways not anticipated by the developers.

b. Businesses and government authorities can influence the realisation of AmI by focusing on trust and usability, which involve concern for privacy and security and intelligent design of the human machine interfaces (HMI).

Relevant issues in this respect are:

- Trust may depend on user-control (interactive computing).
- Usability may depend on provider-control (hidden complexity and proactive computing).

**3. Identify basic trends**

Development of enabling technologies, PETs, autonomic computing, and AmI ecosystems, as well as further development of digital rights management (DRM) and trends in data protection and in civil and criminal liability.

a. Development of enabling technologies: RFID systems, sensor technologies, monitoring networks, behavioural biometric profiling, nanotechnologies.

b. Development of user-controlled Identity Management Systems, Privacy Enhancing Technologies (Privacy Preserving Data Mining, P3P platforms, PKI, Contextual Integrity model Nissenbaum, etc.).

c. Development of autonomic computing and AmI ecosystems.

d. Development of law: DRM, data protection and civil and criminal liability, e.g., for harm caused by autonomic computing.

**4. Identify key uncertainties**

User control, provider control, a balanced combination of user and provider control, as well as developments in data protection.

a. Is user control going to be the paradigm (data minimisation, interactive computing)? Will this result in less intelligence in the environment?

b. Is provider control going to be the paradigm (data maximisation, proactive computing)? Will this result in ignorance and manipulation of the user?

c. Is a fruitful combination possible of user control (interactive), intelligence of the system (proactive), empowering the user by means of minimisation of knowledge asymmetry?

d. Will data protection develop further in the direction of a personality right (human-rights perspective) or will commodification of personal data be explored? Will strict liability for harm caused by automatic profiling be considered?

**5. Construct initial scenario themes**

The central question is: how does the scenario demonstrate the issues Ambient Law is supposed to address? Think of technological embodiment of mandatory data-protection legislation, M2M negotiations about exchange of data for services, history management, and access to profiles.

a. Scenario I could show that proactive – provider-controlled – computing (1) provides comfort if the technologies work properly, (2) provides irritation if the technologies wrongly anticipate preferences, and (3) allows the providers to manipulate user behaviour because it is aware of preferences without the user knowing this. It could also indicate to what extent the user has access to what happens to her data (who stores, sells, buys and uses them), and how a lack of such access effects her (new opportunities and risks are attributed on the basis of profiles the user is not aware of).

b. Scenario II could show that interactive – user-controlled – computing (1) puts a burden on the user, and (2) makes it difficult for the environment to anticipate inferred preferences. It could also indicate to what extent the user has access to what happens to her data (who stores, sells, buys, and uses them how), and how a lack of such access effects her (new opportunities and risks are attributed on the basis of profiles the user is not aware of).

c. Scenario III could show that a right balance between inter- and proactive computing depends on who decides when the user shifts to proactive computing (what is the default position and which are the practical consequences?), on what knowledge basis this is done, and how this interferes with the intelligence of the environment and the possibility of manipulating the user. It could also indicate to what extent the user has access to what happens to her data (who stores, sells, buys, and uses them how), and how a lack of such access effects her (new opportunities and risks are attributed on the basis of profiles the user is not aware of).

## 1.4 Outline

This deliverable provides several perspectives on Ambient Intelligence and the role of Ambient Law in regulating AmI. These perspectives are intended to show why and how Ambient Law is an important direction of thought for AmI development. From a legal perspective, an analysis is made whether and to what extent data protection, privacy, and non-discrimination can be safeguarded in an AmI world, by analysing how the current legal framework for these values would function in an AmI world and where gaps in legal protection are likely to occur. This will provide input for determining the function and scope of AmL. From a technical perspective, it is then argued that the enabling technologies of AmI should be extended with two technical instruments that must play a key role in AmI: Privacy-Enhancing Technologies (PETs) and Transparency-Enhancing Technologies (TETs).

As the combination of technical and legal perspectives shows, AmI has the challenging task of walking the tightrope of both exploiting the technical opportunities of an intelligent environment that seamlessly interacts with users, while at the same time meeting basic normative principles like privacy and non-discrimination. In order to illustrate the pitfalls that threaten policy-makers on both sides of the tightrope, we start the analysis with the illustrative scenarios mentioned in the previous section of two rather extreme possible worlds: a technology-driven, provider-centric environment, and a privacy-driven, user-centric environment (Chapter 2). This sets the stage for the concept of Ambient Law, which we outline in Chapter 3. Then follow the legal and technical analysis of Ambient Intelligence and Ambient Law (Chapters 4 and 5). These analyses, combined with the extreme AmI scenarios, lead us to plead in a concluding chapter for embedding legal norms in the AmI architecture, with a smart combination of provider and user centrism (Chapter 6). To illustrate how this vision of Ambient Law could work out in practice, we end with a third scenario that combines the best of both worlds (Chapter 8).

# 2 Two Ambient Intelligence scenarios

## 2.1 Scenario I: Brave New AmI World

Scene 1: Preparing to work

Tom is 32 years old and is still living with his parents in Stuttgart. He is a financial consultant working for a large corporation. He enjoys travelling and likes listening to jazz and going to the cinema. He has dark hair, brown eyes, and he likes wearing a hat. Every day Tom wakes up at about 7:00 a.m. and leaves home at 7:30 a.m to go to work. Today it is 7:05 a.m. and Tom is still sleeping. Since it is a weekday and Tom has not taken the day off (based on information retrieved by the personnel records in his company) nor is it a public holiday, the system starts playing a track of soft jazz music in order for Tom to wake up. The system detects that Tom moves and a sweet synthetic voice informs him that he should get up so that he is not late to work.

The weather today is rather cold so the system urges Tom to put on his grey costume, which is warmer than the light blue one he has just taken out of his closet, and, since it is rainy, it tells Tom to take his umbrella with him.

Tom left home with an 8-minute delay today, as the sensors in the room reporting inactivity have reported, whereas the rain has caused traffic jams in some streets that are in Tom's daily route to work, based on information retrieved by street cameras. Since Tom must not be late for work, he receives an alarm signal on his Personal Wrist Communicator suggesting to him that he should go to work by metro today. However, Tom moves towards the car to go to work as he is not used to taking the metro, only to find that he is unable to unlock it, since today the sensor at the car lock has been notified about the traffic and blocks Tom's effort to open it. Despondently, Tom takes the metro to go to work. As he has subscribed to the news service, a list of current news is displayed on his mobile device. It includes a car accident in Stuttgart allegedly caused by a software error in the traffic-control system, the stock exchange, a strike at the city centre going to take place tomorrow, a great earthquake in Malaysia, a jazz festival to be held in Munich in 1 month. News such as the elections in Poland, new job positions in the public sector and the glorious start of the new NBA player in the Olympiakos basketball team were not presented to Tom, as they were considered as lying outside his interest by the news service.

Scene 2: His girlfriend's going out

Tom has been involved with Maria, a 29-year-old colleague of his, over the past two years. Maria is making plans with her friends for tonight to go to a new bar in the city centre. Tom will have to stay at work till late in the evening and won't be able to join them. As Maria is having a nice time with her friends at the bar, a man on the other side of the bar – Brian – is staring at her. The bar's system is about to suggest to the barman to give an aspirin to Brian, who must be ill because his brow is covered in sweat and he keeps staring at a single point, when it is corrected by the sensors noticing the rain outside and re-interpreting Brian as being humid with rain as well as being interested in Maria in a statistically significant way. After a while, he calls the waiter and in a few minutes the waiter arrives at Maria's table serving her with a drink and discreetly pointing out Brian. Maria takes the glass in her hand and smiles at Brian. The camera detects the flirting between the two people. Almost simultaneously, Tom receives a commercial ad of the "GetTheCheaters" service at his mobile phone advertising the latest features of the service. Tom is reluctant in getting subscribed to this service, but as he is rather jealous and curious and because the ad is formulated precisely in way to create trust with a person like Tom, he decides to proceed with it. During the smooth subscription procedure, he submits information about his girlfriend, including two photos and personal information, by a single click – his mobile phone automatically selecting the requested information. When Brian is about to leave the bar, he goes towards Maria's table, gives her a piece of paper, smiles, and leaves. Maria has a look at the piece of paper, smiles likewise, and puts it in her bag. The "GetTheCheaters" service sends an alarm to Tom informing him that his girlfriend is flirting with a guy in the bar. In the evening, Maria receives an sms letting her know that "If you like flirting – subscribe now to our Mr Right Radar service", but Maria chooses to ignore it.

Although Tom and Maria do not know it, the personal-relationship services targeting them have been signaled by their employer. The company's employee-watch system calculated that Tom and Maria had low chances of having a successful long-term relationship, and their current affair therefore seems to jeopardise their employee value. By enlisting the system's personal-relationship services, the company hopes that Tom and Maria will sooner realise themselves that they are not really made for each other.

The other morning at work, Tom is quite distant and avoids Maria by telling her that he has much work to do. He seems angry and not sure what to do. The surveillance cameras at work detect his sad and distracted mood and the fact that he makes long pauses staring at the window. Also, the keystroke dynamics monitoring tool at his computer detects nervousness. As the company knows that the employees' mood greatly influences their productivity, it uses the "KeepThemUp" service. Taking into account what happened the previous night, this service concludes that it is difficult for Tom to concentrate on his work. It thus sends him an alarm suggesting to him to go out for a small walk so that he can clear his mind. Tom does not seem eager to move from his office. The service insists and sends more alarms, and the door sensor opens the door. Tom stands up but he chooses not to follow the advice and just heads towards the coffee machine. He selects strong black coffee. The machine however serves him decaf instead. When Tom gets back to his office, he finds a MentalBoost® screensaver message: "Overactive people work better with herbal tea and decaf. Try one!"

Scene 3: At a shop and at the park

Tom has decided to stay at home and relax this afternoon, while Maria is going out for shopping. The surveillance camera at the mall detects that Maria is standing outside a shop and is looking at her watch. The camera infers that she is waiting for someone. Maria receives a message in her mobile phone informing her that the shop named "La Femme" on the same floor has special offers in perfumes. Maria finds this very timely, as when this morning she was about to leave her house, a sensor on her perfume bottle detected that the level of the perfume was low even before Maria herself noticed it.

Suddenly, Brian arrives and they kiss and hug. The "GetTheCheaters" service which is monitoring Maria classifies this behaviour as potentially erotic and notifies Tom that Maria is at the specific mall with a man. It streams a video from the scene. While Maria gets an sms on her mobile phone advertising a romantic coffee corner nearby, Tom decides to go to the mall. As he reaches the place, he receives information in his mobile phone about Maria's current location. She is still with Brian but now in the park outside the mall. When Tom arrives, Maria tries to explain and Tom becomes aggressive towards Brian.

The surveillance camera at the park detects the incidence of violence and an alarm sounds to two policemen who are just some 100 meters away from the scene. The two policemen arrive and they manage to calm down the two men. Automatically, a citizen personal-behaviour profiling system updates Tom's profile with a record of this incident.

Scene 4: Three months later

It has been about two months since he broke up with his girlfriend, and Tom spends really too much time at work, having lost interest in going out with his friends. The camera at work, through the emotion and activity recognition system, detects that he is quite often sad and cannot concentrate. His manager has been receiving notifications about his behaviour, and MentalBoost® messages frequently arrive at Tom's mobile device, proclaiming things like "It is no use crying over spilt milk. Concentrating on your work makes you feel better!". Meanwhile, the sensors at his house have calculated that he spends much more time at home than he used to. Integrating information on Tom from different sectors, such as university records, banks, religion, health and sports records, as well as the dynamically constructed pattern of his behaviour and preferences, a dating service matches Tom's resulting overall profile with others so that it finds potential dates for Tom.

The home entertainment system at Tom's home notifies him that it could find some very attractive matching profiles for girls he could date, but Tom rejects the service indignantly. The next day, the system suggests a side-by-side comparison of profiles: Tom's own archived profile from 5 years ago, when he met Maria; Maria's own profile; profiles of the two best matches the dating service can find; and finally Tom's current profile. Finding such an objective comparison irresistible, Tom accepts to look at these data. He realises that Maria's profile seems to fit his 5-years-old profile much better than it fits his current one. Clearly, he concludes, he has changed over the years, and maybe Maria was really no longer an ideal match for him. The emotion detection system registers his initially cold but gradually warmer reaction to the data he is being shown.

The system now sends notifications to the girls in question that a potential matching profile for them has been detected. As it happens, there is no positive reaction, at least not yet, so the system does not inform Tom about any particular developments.

Scene 5: A few weeks later

As Tom is out for a walk, he passes by a café. Here, Jennie is taking a cup of tea with a friend; she is a single 28-year-old French teacher who attends dancing classes and dreams of traveling all around the world. The system had detected a month ago that her profile matches Tom's well and had notified her, but she had not responded to the profile information. The system assesses that a personal meeting is much more likely to be successful than a display of profile information to each person, so it decides to notify Tom that it's worth going into this café: "A surprise may be waiting for you in this café! Click here for a clue." Tom decides to ignore the clue and simply go inside the café to see what the future has in store.

Jennie has in the meanwhile received her daily horoscope advising her to look out for handsome dark-haired men wearing a hat. Just when she finishes reading the horoscope, she looks up, exactly in time to see Tom entering the café.

## 2.2 Scenario II: Users at the Buttons

Introduction

David Cragg is a 39-year-old humanities teacher and housemaster at a British public school in Royston

Vasey, in the north of England. He first met his now wife Li-lian (née Cheung) while holidaying in mainland Greece. Li-lian's family are originally from Hong Kong, but she is second generation in the UK. Having planned their wedding some 12 months earlier, the Craggs are now on honeymoon for two weeks in Crete. This, due to circumstance, coincides with the imminent delivery of their first child whose announcement came as a 'happy surprise' some months earlier.

Scene 1: It's all Greek to me

Their late arrival at 'Hotel Warwikakis' in the city periphery the night before had, on the whole, been uneventful. David had previously opted not to allow his intelligent home to send a public version of his family preferences agent to their hotel in advance, and instead accepted that because of this they 'may not be able to provide for all specific needs on the first night'. However he hadn't figured on the Greeks being a little slow on the uptake of new technology, and so despite trying to use his MyComm personal communication device to upload the data at the reception desk, he found he was unable to because their system did not use the latest international standard.

Despite this, after converting the profile agent to an older format and answering a few questions related to the types of personal data the hotel was allowed to read from their agent and for how long they wished their preferences to be stored by the hotel, they enjoyed a room lit and heated to their approximate preferred comfort levels, classical music piped through the suite's music system, and the television channels ordered to reflect their tastes.

After a good night's sleep, the day had started abruptly at 06.45 by a wake-up alarm call. Unfortunately neither David nor Li-lian wished to get up at that time, but during the conversion to the older format, the MyComm had been switched out of holiday mode, and as such had assumed today was like any other typical working day. This was rapidly rectified.

Some time later, after getting out of bed, Li-lian decides that she is too exhausted to venture outside that morning, so she opts to stay at the hotel while David does some sightseeing. As part of Li-lian's travel-insurance policy, she is wearing a MediCheck health-monitoring system which monitors her continually for anomalous physiological changes. David ensures that his MyComm device is listed to receive alerts, and authorises the device to contact the hotel reception in the event of an emergency. As is default with such devices, in line with Greek law, the local emergency service is authorised automatically to be contacted.

Scene 2: Meeting the local location services

David was never one for shopping, but when away always has a look around the local shops. Like many cities, the centre is littered with international clothing stores, most of which use RFID tag scanners in the doorway so as to scan for tags in clothing and accessories to work out what the customer wears and thus to create a rough profile of them. Additionally, most shops welcome the ad hoc automatic upload of shopping agents from personal communicators so as to create a list of offers and discounts to help tempt the customer. By default, David has such options disabled on his MyComm device, and having felt a sense of personal invasion when, for example, the shop is able to alert him to discounts on his type of underpants based on the RFID tag data, he opted to subscribe to an online tag-swap site which periodically sends him credit-card sized plastic tokens stuffed full of random RFID tags designed to confuse the shop's profiling agents. His favourite one apparently registers him as wearing a sombrero and carrying eight kilos of jam.

After a bit on an amble around the local area, David wants to find some food. Having heard of the local dolmadakia, he is interested in trying them, but he also has some dietary requirements that he needs to be wary of. David's MyComm device is a 5th-generation mobile device with many useful functions and access to location-based services. One of his favourites is the locator service which enables the device to pin-point his location and seeks out places of interest to him – in this case restaurants. David's device is also equipped with MInD, a mobile device identity manager which allows him to specify a range of partial identities which he can use when accessing such online services. David enables the service and selects restaurant finder. Then he selects his 'personal food finder' profile which stores details of his dietary requirements and then selects 'local food' and 'time sync', which tells the service to look for items relevant for the current time. After a few moments, the MyComm indicates that the service is requesting further details – in this case his location. David authorises the transfer and a list of appropriate places appears on the screen. David is also notified by his device that he can update his iConcert database via the same service provider using the information he has already sent. iConcert is a plug-in for his MyComm that monitors his music library and generates a personalised list of upcoming concerts in his local area. The filtering of relevant events happens on his local device, so that no further information is needed by the service provider. He chooses not to bother, so he remains unaware that his favourite sitar player, Ravi Shankar, is performing with the Cretan lute-player Ciborgakis in the city just that night.

While en route, David's MyComm informs him that he is carrying insufficient cash funds to get him through the day after a typical breakfast at the restaurant. David is aware of the link between uses on his eComm card and subsequent targeted mailings from his card company's 'trusted group of associates' (a downside of the agreement that assures him a marginally decreased interest rate), and his profiling agent knows that he usually opts to use cash for smaller one-off purchases. As such, a detour to a cash-machine is offered and accepted, after David has authorised his MyComm to give his name and nationality to the local ATM finder service. Cash-machines still use PIN security, but this is augmented with additional biometric protection. However, rather than using non-revocable biometrics such as fingerprints, the cash machines use a type of keystroke analysis to obtain a characteristic typing pattern from the PIN button presses. This type of changeable biometric has become widely accepted as preferable. David is annoyed when he has to type in a sample line of numbers four times over and is still rejected by the machine. He now has to use the fall-back option of authorising the ATM to make a picture of him and compare this to the facial-biometric template stored by his UK bank. Even though he knows the picture will be stored for five years by the hefty Greek anti-identity-fraud laws, he has no choice but to accept.

Scene 3: I don't drink coffee, I take tea my dear

Because it's a holiday, David doesn't bother with trying to find out the Greek menu by himself. He uploads his profile to the restaurant system and clicks his agreement with the system's data-processing practices. He is guided to his preferred seat position in the window and is able to select his meal from a heavily customised menu. He enjoys the luxury of just seeing his favourite foods fulfilling his dietary requirements offered to him on the menu, even though he knows the restaurant will sell his data to many food-broking services. The restaurant is augmented with sensor technologies and in the absence of any other information, makes sweeping generalisations in order to project targeted advertising on the menu card when not in use. David is not best pleased to find an advert for a local sports club appear as a result of the doorway height sensor and stool strain sensor concluding he is too heavy for his height. This is soon updated when he removes his rucksack and his weight is recalculated. Unfortunately, being a result of a combined group profile of the current restaurant patrons, changing the music of 'Sakis Rouvas' which is piped through the building is not so easy to correct.

After a delicious assortment of mezes, and the best part of a drink, the waitress, alerted as to the volume of drink remaining by the cup coaster, comes over with a filter coffee pot to offer a complimentary top-up. Unfortunately even the advances in Ambient Intelligence haven't eliminated human error, and David explains just too late how he had actually gone out of his way to find Lapsang Souchong tea . . .

While preparing to leave, a message comes through the MyComm from David's intellifridge back at home. It requests his acceptance for a menu for that evening's meal based on items that are nearing expiry in storage. Usually, the fridge would negotiate such a message with the house gateway, and thus discovered that the house had gone into holiday mode. However, David had previously configured a link with it in order to interrogate it directly, so messages were unfiltered. He starts to remotely configure the preferences to route it back through the house and avoid further messages when a priority message appears – Li-lian's MediCheck device has found cause for concern.

Scene 4: Congratulations, it's a…

Despite having had several false alarms in the past, this time Li-lian was in complete agreement with the MediCheck device – something was definitely happening! Having automatically alerted the concierge's desk and contacted the local emergency services, help was quickly to hand, and within 30 minutes, Li-lian was being wheeled through the doors of a maternity unit. Having been largely planned in advance by her insurance company, her arrival was not totally unexpected. Indeed, her doctor had already authorised access to relevant portions of her e-medical file to the hospital.

However, in her haste in leaving the hotel, Li-lian had only taken her Chinese ID card with her. Unfortunately, this has led to some confusion over her identity because her Chinese name differs from her English name, and to further confound matters, her recent change of surname has already been updated on her e-medical records. Fortunately, Li-lian is still alert enough to give her consent to the hospital cross-referencing her iris scan with that stored in the medical files, and her identity is confirmed. She realises that she had better change her e-medical preferences to allow such identification without her consent, seeing the kind of emergencies that can arise, particularly when traveling.

Meanwhile . . .

David returns to the hotel too late to see Li-lian, but, having taken the opportunity to collect some of her belongings for her stay in hospital, he heads to the hospital in their rental car. Not being familiar with the local area, he instructs the on-board GPS unit to guide him to the city hospital, and for once, he doesn't mind at all that his personal data and profiles are being transferred to the local rental-car company in exchange for the routing service. Being slightly flustered and concerned for his wife, David becomes increasingly annoyed with the enforced limits on the car, and so he disables the overrides by putting the car in 'emergency mode'. Unfortunately, the traffic monitoring cameras observe his erratic driving, trace the car back to the rental company, and automatically issue a fine to David. As a result, David is also has levied an additional sum onto the car insurance policy by the rental company.

On arrival to the hospital, David makes his way inside, and looks for directions to maternity. Because most of the signage is in Greek, he uses the camera on his MyComm device to translate the words to find his way. He curses when his MyComm only yields error messages and he has to spend precious minutes to use sign language with a passing nurse to indicate where he wants to go. Sometimes, he feels there are distinct advantages to living in the US, where buildings automatically infer and smoothly indicate people's desired routes. The European AmI Directive, however, has prohibited such automated guidance without explicit individual consent. Who cares for explicit informed consent when your wife is in labour?!

The maternity unit is augmented with additional security measures to prevent unauthorised personnel from entering. To request access David, is asked to scan his iris, and not being on the list of personnel is told to wait for further instruction. Security at the hospital is tight, and the security department is able to cross-check iris scan patterns with the European centralised biometric database. Despite having been acquitted of an alleged offence with a minor at a previous place of work, David's details are still to be found in the database, and as such he is taken aside for further questioning as to his purpose at the hospital.

After some four hours in labour, Li-lian gives birth to a healthy baby girl. As has become standard, the baby is implanted in the umbilical stump with an RFID tag to allow identification in the hospital. Although such temporary implants have become normal practise, permanent implantation is left for the parents to decide at a later date. David and Li-lian have already decided to have the umbilical tag removed, even though they realise that younger generations seem rather fond of these identifying implants. Zoe – as the girl is named – will just have to decide for herself when she comes of age whether or not she wants to be permanently warwicked.

# 3 A vision of Ambient Law: Conceptual Exploration

## 3.1 Law and technology

There are different ways to understand the relation between law and technology:

a. law as set of prescriptive rules and technology as an instrument of their implementation;

b. law and technology as interchangeable instruments of regulation;

c. law as a body of authoritative normative incentives, embodied in rituals, orality, the script, printed codes or other types of technologies.

The idea (a) that a technology is a mere means to implement the law is prone to mistake technology for a neutral tool. In reality, technology, though neither good nor bad, is never neutral (Kranzberg 1986), as it has an unmistakably normative impact on those using it. The idea (b) that law and technology are interchangeable instruments of regulation opens the possibility to short-cut democratic procedure, because contrary to law, technologies do not, generally speaking, require legislative effort. To understand the idea of Ambient Law (AmL), this must be kept in mind, as it presumes another relationship between law and technology, as formulated in (c). Historically, law has always been embodied in one technology or another. In fact, the transformation of oral law via written law to printed code has fundamentally changed the scope and the nature of law. Law as we know it today is unthinkable without the advance of the printing press at the beginning of modernity, and the move from printing press' letterisation to the digitalisation of information storage and communication will again have a major impact on the next stage of the law.[7]

This is not to say that all of the law will now be AmL. Modern law depends on the printing press, but we still speak of written law and unwritten law, even if this cannot be equated with medieval law or law in non-state societies. Our interest in Ambient Law derives from the lack of efficiency and effectiveness of contemporary data-protection legislation as embodied in printed code. This ineffectiveness erodes the legitimacy of data protection and may nourish distrust of emerging technologies. The ineffectiveness of data protection finds its climax in the face of the vision of Ambient Intelligence, based on real-time profiling of things, people, movements, and states (temperature, humidity etc.). Ambient Intelligence involves a shift from interactive to proactive computing, and this in itself seems to solidify a loss of user control, however comfortable the user may feel in her customised environment. To regain some measure of transparency – a necessary precondition for control – new technologies will have to be developed that reveal which profiles are inferred and applied, and what the consequences are in terms of the risks and opportunities attributed to categories of users.

In the following section, we will briefly refer to the technological embodiment of pre-modern law, explaining some of the consequences of the move to the printing press and modern law. This will form the prolegomena to a conceptualisation of the embodiment of law in the emerging technologies that nourish AmI, which constitutes Ambient Law.

[7] Letterisation refers to the use of the phonetic alphabet which allowed the movable type printing press (using only a limited set of letters to create an enormous amount of texts). Pictographic or ideographic alphabets could not work with such a small set of recombinable elements. Digitalisation – based on a set of two signs – has again revolutionised the scope of communication and information (think of hypertext, use of images).

## 3.2 The technological embodiment of law

### 3.2.1 From oral to written law

A society based on oral communication depends on face-to-face contacts, spoken language and artefacts in a shared Umwelt (Jiang 2002, Blavin and Cohen 2002, Goody and Watt 1963, Ong 1982). Language can represent what is not present in the immediate here and now, but in order to sustain and hold together a people, oral law depends on individual human memory. Mnemonic techniques and highly ritualised exchanges embody the normativity of oral law. The only way to sustain a legal tradition from one generation to the next is to store the way things should be done in the long-term memory of those who share jurisdiction, having no access to external storage like clay tablets, papyrus scrolls, or the pages of a book. Because of the need for face-to-face communication to establish and re-establish what counts as the law, jurisdictions are small: polities do not exceed a certain number of people, due to the limited means to create a shared understanding or common sense (Eder 1976, Wesel 1985).

Once the script enters the picture, it becomes possible to write down the law for people one will never even meet: the inscription allows communication beyond the context of the author of the law. Trans-local and trans-generational law can now generate a community of people who may share little else than a common law, enacted by a king or an emperor who has instructed his officials to spread the same – written – law across a vast territory. To keep a grip on such a vast polity, the king will be modest in the claims this law exercises over his people, by leaving them their local, unwritten law for the settlement of local conflict. But the written law does enable him to register people for the purpose of taxation and subscription, which form the backbone of the emerging state, together with royal or imperial jurisdiction (Scott 1998, Torpey 2000, Caplan and Torpey 2001).

The move from oral to written law thus affects (Hildebrandt 2002, 2008, Ricoeur 1992, Lévy, Goody and Watt 1963, Geisler 1985):

- distantiation of meaning: material fixation of legal rules;
- distantiation of the author: loss of control of the author over the meaning of the law, creating the need for interpretation;
- distantiation from face-to-face communication: establishing non-ostensive reference;
- distantiation of the public/audience: creating the possibility to form large trans-local communities.

### 3.2.2 From written law to modern law

The move from (hand)written law to printed code is as revolutionary as the move from orality to the script. As Eisenstein (2005) and Lévy indicate, the age of writing necessarily centers around a limited amount of primary texts, which are commented upon in subsequent centuries. The advent of printed matter extended the scope of texts to be read, initiating an era of proliferating cross-textual reference, creating a knowledge explosion that was previously unthinkable. This proliferation called for some kind of categorisation to keep track of the overdose of available information. Besides the fact that the material fabric of printed matter ('letterisation' in terms of Lévy) implied some kind of standardization (Eisenstein 2005:56-70), the sheer quantity of available texts initiated a process of rationalisation, codification and cataloguing of information.

The impact of all this on law cannot be underestimated. The manuscript of a hand-written law needs to be copied by clerks to reach its full audience, and one is never sure that no mistakes have been made; in contrast, 'letterisation' seems to rule out mistakes (or enlarge them as the mistake is repeated), easily creating a community that is now effectively bound together by the same unified text. This first enabled the rule *by* law, providing kings and emperors with an unprecedented consistent rule over their subjects, kept in line by a bureaucracy of civil servants obliged by identical royal instructions. Modern law – the condition of possibility of the modern state (Berman 1983) – owes its reach, efficiency, and effectiveness to the transition from hand-written common law and enacted decrees to full-fledged codes as they emerged at the beginnings of modernity (16th-18th centuries), coming of age in continental 19th-century national codifications. Codification differs from mere statutory law in its systematic approach of an entire legal field (private law, criminal law, administrative law). Especially in the continental European legal tradition, one can detect how the proliferation of legislation called for a categorisation of the sources of the law, initiating a strict hierarchy between different sources, in order to prevent a chaos of authoritative texts. At the same time, the need for interpretation that arose with the transition from orality to script is reinforced to an unprecedented degree, creating the need for a highly complex body of doctrines to prevent interpretation from running amok. So, the printed code was a fierce instrument in the hands of those who governed their subjects, allowing a detailed control of their lives. It thus initiated the birth of the police states of the 18th and 19th centuries and was a trailblazer of the 20th-century welfare state.[8] However, the same need for reiterative interpretation and the same growing distance between author and addressees of the legal codes facilitated the birth of the rule *of* law and of constitutional democracy, with its emphasis on individual liberty, plurality, and contestation of the rule of government. The volatility of all interpretation created the middle ground for citizens to contest dominant interpretations in a court of law, thus providing the means to speak truth to power.

In other words, the move from hand-written to printed code thus effected:

- proliferation of legal texts, increasing the need for interpretation,
- resulting in a quest for legal certainty
- to be provided by:
    - systemisation of enacted law: codification;
    - systemisation of the interpretation: doctrine;
- rule by law:
    - of a sovereign over his subjects,
    - unifying enacted law over a vast territory;
- rule of law:
    - the author/authority of the law cannot entirely determine its interpretation;
    - dominant interpretations can be contested in a court of law (separation of powers).

[8] The term police state historically depicts the absolutist states of 17th and 18th century Europe, see e.g. Von Mohl 1866, Chevallier 1994.

## 3.3 From modern law to ambient law?

### 3.3.1 From letterisation to digitisation

The move from oral to written culture did not always involve letterisation or the use of the alphabetic script. Many ancient civilisations developed pictographic or ideographic scripts, which were much harder to translate into letterpress printing. Chinese ideographic script, for instance, was printed by means of woodblock prints, not capable of constituting on the basis of a limited set of letters an unlimited set of words, sentences, paragraphs, chapters, and books. So, even though the printing press flourished in China long before Gutenberg invented letterpress printing (Reinhardt 2005), it did not entail the revolutionary effects discussed above. Though woodblock printing enlarged the scope of written text, it did not entail the kind of proliferation of printed texts flooding the mind of European lawyers.

The recent emergence of digital code as the latest revolution in communication technologies (after orality, the written script, the letterpress, and – we may add – mass media) again entails major shifts in the way society is organised. For the sake of the argument, here are just three witty reminders of the speed with which everyday interaction is changing – which should not surprise anybody who talks with their parents or grandparents:[9]

> I once received a fax with a note on the bottom to fax the document back to the sender when I was finished with it, because he needed to keep it.
>
> Customer in computer shop: “Can you copy the Internet onto this disk for me?”
>
> Customer: “So that'll get me connected to the Internet, right?” Tech Support: “Yeah.” Customer: “And that's the latest version of the Internet, right?” Tech Support: “Uhh...uh...uh...yeah.”

The first *witz* reminds us of the fact that digitalisation has created a proliferation of copies that change the nature of concepts like 'theft' (e.g., in the case of data and music), calling for new measures of protection in the field of intellectual property, security, and privacy. The second and third *witz* remind us of the dynamic, ever-expanding nature of the Internet, moving from text to hypertext, from content to relationship (from semantics to syntaxis), from correspondence to reality to the creation of virtual realities with effects in the real world (from semantics to pragmatics). Accumulation of texts that build up into a comprehensive system is no longer necessary, nor feasible. The sheer volume of potentially relevant texts to which one has instant access and the possibility to surf right through them via hyperlinks, creates a need to develop pattern-recognition (profiling) technologies, without which one will be flooded by information that ends up as noise.

If the vision of AmI is realised, the off-line world will be turned online, and many of the features of cyberspace will invade and transform ordinary space. Summing-up cyberphilosopher Pierre Lévy, a transition can be detected:

- from a linear sense of time to segments and points;
- from accumulation to instant access;
- from delay and duration to real time and immediacy;
- from universalisation to contextualisation;
- from theory to modelling;

[9] These jokes are cited at http://jmm.aaa.net.au/articles/6929.htm.

- from interpretation to simulation;
- from semantics to syntaxis and pragmatics;
- from truth to effectiveness;
- from stability to change.

Following his line of thought, we may expect new paradigms in law, e.g.:

- from the careful study of legal texts from beginning to end to the screening of cross sections to find relevant patterns (using profiling technologies);
- from compilations of authoritative texts, selected by authoritative scholars and judges, to instant access to all the sources of the law (legislation, case law, doctrine), flooding us with data to an extent beyond our capacity for comprehension, calling for profiling technologies to distinguish noise from information;
- from the delay and hesitation inherent in procedural safeguards that build on reflection to real-time autonomic decision-making by means of jurimetric technologies;
- from the ambition to achieve equal application of general legal norms to equal cases to a personalisation that comes close to 'Einzelfallgerechtigkeit' (the notion that justice is established for each and every single case);
- from the complex theoretical constructions of legal theory to pragmatic legal modelling;
- from hermeneutic practice of law, based on the need to interpret the sources, to a pragmatic practice of law, based on the need to anticipate future impacts;
- from an emphasis on the meaning of legal texts to an emphasis on the legal consequences of their application;
- from an emphasis on legal certainty, intra-systematic coherence, continuity, and stability (legal doctrine and jurisprudence) to real-time adjustment to a rapidly changing fluid world that needs permanent real-time monitoring instead of the slow construction of durable knowledge that is universal and survives the ravages of time.

### 3.3.2 From printed code to digital code

The advent of printed legal Codes (like the Code Civile or the Code of Criminal Procedure) called for rationalisation and stimulated the construction of hierarchical systems of law. Digital Code, or computer code as a kind of Law (Lessig 1999), may lead to networks of overlapping codes that negotiate their application. This move from system to network, from imperative to negotiated authority, may be complemented with a move from creative application of the law, based on human interpretation, to mechanical application of the law, based on M2M communication and real-time monitoring (modelling, simulation, feed-back and implementation).

Printed codes in the end terminated the reign of the literate class, allowing everybody to become literate, to participate in the creation of law (democratic legislation) and to contest the application of the law in a court of law. This way, printed codes have been a precondition for the rise of constitutional democracy as we know it today. Digital code, however, seems to introduce a new 'literate' class, creating at the same time a class of computer illiterates.[10] This can be illustrated by referring to the case of Ambient Intelligence, where the idea is that technological (digital) complexity is hidden, to make life easier for the user, which enlarges the gap between illiterate users and knowledgeable providers.

If digital code is naïvely understood as (a) a neutral tool to implement the law – e.g., by using DRM to enforce intellectual-property rights without paying attention to the impact of such implementation for 'fair use' – then the normative impact of the technology itself is hidden, which may have serious consequences for the scope and the nature of law in AmI environments. If digital code is naïvely understood as (b) just another tool for the implementation of government policies – exchangeable with legal instruments depending on their foreseen efficiency and effectiveness – then the specific constraints of constitutional democracy can be bypassed at will.

For this reason, we must acknowledge the fact that for Ambient Law to be effective and legitimate it must be understood as (c) the technological embodiment of legal norms, requiring democratic legitimisation as well as the possibility to contest its application in a court of law. While these two requirements of law in a constitutional democracy are taken for granted in a society based on printed code, we may have to reinvent them in the case of digital legal codes.

## 3.4 Legal constraints for AmL in a constitutional democracy

To count as law in a constitutional democracy, two fundamental requirements must be met:

- the creation of law is initiated by a democratic legislator, and
- its application can be contested in a court of law.

In fact, technological articulation of legal norms in a constitutional democracy demands specific checks and balances at three different levels:

- the level of legislation (which is both legal and political). At this level, the use of specific technologies to support or enforce legal rules needs democratic legitimisation and needs to fit constitutional demands;
- the level of administration (which is both legal and executive). At this level, the use of specific technologies to support or enforce legal rules needs to comply with the principles of fair and transparent administration;
- the level of adjudication (which is legal, political, and executive, because it determines the scope of the law). At this level, the use of specific technologies to support or enforce legal rules must be made contestable.

For Ambient Law – a law that effectively protects and facilitates interactions in an AmI environment – these requirements will have to be taken into account when developing the concept of AmL, when preparing statutes that embody AmL and when building the relevant prototypes.

Altogether, this means that AmL is NOT:

- just the autonomic application of legal rules, or

[10] While almost everybody who votes (for the legislature) can read and write in our part of the world, not everybody who suffers or enjoys the consequences of ICT can read or write computer code.

- an alternative for legal rules.

Rather, AmL is:

- the embodiment of legal rules in the emerging technologies they aim to regulate.

## 3.5 Provisional vision of Ambient Law (AmL)

Three notions are important for fleshing out the concept of Ambient Law. A central notion is 'law by design'. In addition, two other concepts seem to have a high potential for developing the notion of AmL: Helen Nissenbaum's concept of contextual integrity and IPTS' concept of digital territories. These notions will be briefly explained in this section.

### 3.5.1 Law by design

An interesting development within the ethics of technology is the idea of 'value in design'. It basically refers to the fact – already discussed above – that technological artefacts are neither good not bad, but never neutral. This is the case because they actually influence the types of behaviour we (can) develop, and this may have moral implications. Because technologies can be designed in different ways, having a different impact on our behaviour, their moral significance will vary, depending on the design (Flanagan, Howe et al. 2007). One way to take responsibility for the moral significance of a specific design is to integrate design choices into the legal process, enabling democratic procedure to determine the way technologies steer our behaviour. One could thus understand Ambient Law as a type of 'law by design'.

This would imply that AmL articulates specific legal norms in the relevant technological devices or infrastructure. If we focus on the norms that aim to protect citizens against violation of their privacy, while empowering them by providing transparency rights, we could ask the legislator to require that the mandatory rules of data-protection legislation (transparency, use limitation, purpose specification, consent, data quality, participation, accountability of the data controller) are *inscribed* into the architecture of AmI, *making the violation of these rules difficult by means of design*. One could even say that whereas modern law (based on printed code) separates the written code from its implementation, this is not necessarily the case with AmL. This could mean that the law is not only more effective but also more equal in its application.[11]

For instance:

- **transparency:** history management of one's personal data and access to processed personal data with data controllers should be made possible via M2M communication;
- **purpose specification & use limitation**: such transparency should enable one's PDA to check (M2M) which purposes are specified, and to check whether the principle of use limitation has been complied with in light of these purposes;
- **consent**: one's machine-proxy (the PDA that serves as a proxy when negotiating consent) should be capable of negotiating, e.g., the supply and processing of personal data,

[11] It may appear that modern law has general application, while AmL only applies to those who use the technology. This not the case. Most legal rules address categories of citizens: e.g., employers, road-users, fathers. AmL would address those who use the technology against which AmL aims to protect them. In that sense its application is more general, because in the case of written law the application depends on the actual implementation. We repeat that 'automatic' application of legal rules presumes adequate checks and balances to count as legal rules (democratic legitimisation and contestability in a court of law).

according to one's personal preferences, while taking into account the mandatory aspects of data-protection legislation;

- **data quality & participation**: one's machine-proxy should be capable of matching data stored in data bases with one's accurate personal data, and be capable of requiring adjustments if data are not correct (anymore);
- **accountability of the data controller**: at all times, one's machine-proxy should be capable of *identifying* the data controller who reads, collects, stores, or otherwise processes data, including all others that have access to these data; this could be done pseudonymously, as long as there is identifiability of the data controller in case of data-protection violations.

As argued in FIDIS deliverable 7.7, present data-protection legislation lacks adequate protection against the application of profiles, especially because citizens are not aware of the consequences of such application. This would require a new right of access to such profiles in order to empower citizens to contest the way they are being categorised, irrespective of whether these profiles have been derived from their own or others' (personal) data. Such a right has no meaning if the technological infrastructure that enables AmI does not provide the technological means to achieve such access, or when it lacks user-friendly human machine interfaces to allow citizens to understand the profiles and how they can impact their lives. For this reason, FIDIS deliverable 7.7 argued for TETs: transparency-enhancing (legal and technological) tools. The concept of TETs can of course refer to transparency of the processing of personal data, but in relation to AmI and profiling we emphasise the need to develop TETs to make profiles transparent that may be applied even if they do not fall within the scope of the concept of personal data. Both TETs and privacy-enhancing technologies (PETs) could be examples of AmL in as far as they become integrated into the legal framework, combining a right to privacy or transparency with the technological inscription of the right into the AmI infrastructure.

We could paraphrase the above as follows: Ambient Law in fact **uses the technologies** that data protection aims to regulate while protecting against their undesirable consequences, **in order to facilitate this protection**. This may sound like a paradox; indeed, it is quite similar to the famous paradox of the 'Rechtsstaat': protecting citizens against the state by allowing them to contest actions of the state in a court of law, which shares the authority of the state itself.

In Chapter 5, the state of the art regarding the technological implementation of mandatory parts of data protection is further discussed.

As to transparency rights concerning the application of profiles, major issues arise in the context of cooperating objects in networked environments that allow real-time autonomic profiling in order to seamlessly adapt the environment to a user's anticipated preferences. The technological articulation of a legal right of access to profiles is still a challenge, as such technologies have not been developed yet. In FIDIS report D7.7, we have argued the need to develop transparency-enhancing tools (TETs), integrating legal and technological tools to prevent:

- unfair discrimination (unfair due to the fact that citizens are not aware of who knows what and who decides on which basis);

- the autonomy trap (refined segmentation allows manipulation whenever the user is not aware).

### 3.5.2 Nissenbaum's contextual integrity and its operationalisation

When elaborating the concept of 'law by design' we may need more detailed definitions of concepts like privacy, transparency, and profiles. To articulate the legal norms that protect values like privacy, autonomy, and non-discrimination, we will need semantics that can be translated into machine-readable data. At the same time we must prevent static a-contextual definitions, because core features of AmI are flexibility, mobility, and contextual adaptation. For this reason we may turn to Helen Nissenbaum's concept of 'contextual integrity' (Nissenbaum 2004), which can serve as an example of how to rethink legal notions in order to make them robust in the face of emerging technological infrastructures.

An important consequence of turning the offline world online will be a further transformation of the borders between the public and the private. By introducing the notion of 'contextual integrity', Nissenbaum avoids the need to separate the private sphere from the public sphere, and we would argue that an AmI space will require safeguards against a violation of 'privacy in public'. The vision of AmI implies a series of enabling technologies, like sensors and RFID, that will be used as surveillance technologies that are capable of making people transparent in their public behaviour, thanks to profiling techniques. Both government agencies and commercial service providers (as well as public-private service providers in the sphere of, e.g., health care) will develop extensive monitoring infrastructures to be able to deliver real-time adaptations of the environment. For this reason Nissenbaum's dynamic concept of 'contextual integrity' is promising, compared to the notion of privacy (which is too easily restricted to the private sphere). To prevent a violation of a person's contextual integrity, Nissenbaum claims the relevance of two types of norms:

- norms of the *appropriateness* of a specific information flow, and
- norms of flow or *distribution* of information.

By articulating such norms *as legal norms* into the technological infrastructure of AmI, we could perhaps find ways to make the opposing paradigms of proactive computing and personal autonomy compatible. The violation of privacy would depend on the context and refer especially to a potential disruption of power (knowledge) balance, which could develop between individual citizens and the service providers that process data and apply profiles. It would require an intelligent mix of sensitivity to context and foreseeability, combining dynamic interpretation with the robustness of legal certainty. In law and legal theory, such a combination is not very surprising: fundamental concepts like privacy are essentially underdetermined, having an open texture in need of permanent fine-tuning to changing circumstances.

The concept of appropriateness is relevant for fair information-processing principles like purpose specification and use limitation, providing the rationale for the interpretation of such principles. For instance, instead of demanding that all purposes are always specified and the use of data always limited to the declared purpose, norms of appropriateness would require of the purpose to be appropriate, taking into account the specific features of the context within which the data are exchanged with special focus of the consequences of the processing of data in terms of profiling and categorisation.

The concept of distribution is especially relevant in the case of transparency rights, again providing a rationale for the application of such rights, taking into account the reciprocity between data subject and data controller.[12]

Nissenbaum's concept of contextual integrity thus seems promising as a means to create a middle ground between the opposing paradigms of data minimisation (as a means of user control) and data maximisation (as a means to achieve a smart environment):

- the flow of information is not unlimited (not every exchange of data or profiles is *appropriate*), and
- the transparency of consumer-citizens is countered by transparency of profiles (the flow of information is reciprocal, generating a fair *distribution* of knowledge and information).

In fact, Nissenbaum has made her concept of 'contextual integrity' operational by formalising it in a framework of temporal logic, thus articulating norms for the exchange of data into the technological architecture (Barth, Datta et al. 2006). She thus provides an interesting example of how to inscribe a normative framework into a technological infrastructure, which may clarify how AmL should be designed.

### 3.5.3 IPTS' D1gital Territ0ries concept – an overview

As discussed extensively in several FIDIS deliverables (D7.3, 7.4, 7.5, 7.7), the legal regulation of informational privacy often proves to be inadequate to ensure the protection of our privacy and personal data in the digital space, since sometimes it cannot be enforced adequately or cannot keep up with rapid technological developments and social changes.

In this context and to address these considerations, the European Commission's Institute for Prospective Technological Studies (IPTS) has engaged in research towards developing a concept that would allow individuals to manage distance and boundaries, the 'territories' in this new space, in a social and legal sense, while also providing a proper balance between security and privacy.[13] Although the issues are not always that clear, people have learnt to become aware of the boundaries between physical and digital space and act accordingly.

At this point, the D1gital Territ0ries (DT) concept is brought forward to provide an appropriate way to protect privacy and personal data in the digital world, while promoting freedom of expression and enhancing collaboration and communication in public places of the digital world. Because law in a constitutional democracy is involved in empowering citizens to create, shift, and sustain borders in order to develop and sustain their personal identity (self), the concept of digital territories compares well to Nissenbaum's contextual integrity and may be presented as a second example of how to rethink law from the era of the printed script into the digital age.

[12] Cf. the principle of reciprocity introduced by Roussos et al. in the context of mobile identity management, see Roussos, Peterson et al. (2003). In FIDIS deliverable D11.1, this principle has been introduced to check the power (im)balance between user and service provider. See also Jiang 2002.

[13] Daskala, B. & Maghiros, I. (2007), *D1gital Territ0ries - Towards the protection of public and private space in a digital and Ambient Intelligence environment.* IPTS EUR 22765 EN. Available at: http://www.jrc.es/publications/pub.cfm?id=1474.

The idea of 'territory' has been present in the physical space almost as long as human presence on earth. Legal rules and tacit socio-cultural norms and even traditions constitute the guidelines for people's understanding of what is private or public space or of what is socially accepted as private or public space. The fenced land, the 'keep out' sign on someone's private lawn, the questioning look and cold stare given to strangers in a neighborhood bar, are just a few examples of the 'intuitive validity of the idea of territory' in the physical space; territorial behavior basically aims at achieving a desired level of privacy.

Daskala and Maghiros have identified the following three different types or layers of digital territories, according to the degree of control that individuals exercise over their data in the specific space and the relative duration of the individuals' claims to the space.

- **Primary or Personal DT** – The primary digital territory regards a person's digital personal space. This space encompasses the individual's digital identities as well all digital personal data of a person, including any data which are generated by the person's on-line activities. As such, the personal DT aims at achieving a desired level of privacy, while allowing the performance of any number of selected everyday tasks.

- **Secondary or Group DT** – This type or layer of DT is a hybrid, as it combines both the total and pervasive control allowed to participants in primary territories and the almost-free use of public territories by all persons. It basically regards groups of individuals that share common interests or purposes; hence, it is also referred to as a group DT. The secondary or group DT has elements of public access, considering that it is 'used' by two or more persons, but at the same time, its owners enjoy a certain degree of control, albeit not to the same degree as over their personal DT. A characteristic example of this type of DT is the future smart home or the workplace environment.

- **Public DT** – Any individual has free access and may exercise a low level of control in the context of a public DT. It is a kind of 'commons' in digital space, a free territory, open to the society members at large. In the physical, space it could be for example a beach, a street or a park; in the digital space, it is for example a non-moderated on-line forum, or a publicly available digital space such as an on-line newspaper offering space with individuals' comments.

Apart from the types or layers of the DT, Daskala and Maghiros have also identified four basic components of a DT that are necessary in order to enable a functional DT: bubbles, borders, markers, and bridges.

- **Bubble** – Firstly, the (digital) *bubble* is a dynamic personal info-sphere, or better data-sphere, since it basically 'holds' the person's personal data, and is used to set the borders, restricting or allowing data and information coming in or going out of it. The notion of bubble encompasses all the interfaces, formats, rights and agreements, etc. needed for the management of personal data and informational interactions.

  The size of the bubble may vary as a result of its information content, the form of interaction the individual wants to perform, and the overall 'trust' assigned to the environment of the interaction. Using a cell-membrane analogy, the bubble has a two-way exchange with the environment, sometimes from the inside of the cell out to the environment and sometimes from the environment into the cell.

- **Borders** – The second component of a DT, the *borders*, are seamless, fictitious lines that draw its perimeter, implementing the permissions set through the bubble. Therefore, these borders are always under negotiation and they adapt to different situation or spaces; they are also not autonomous but are set by the bubble. They thus change, decrease, or increase according to the 'will' of the bubble, and the boundaries that it wishes or is obliged to set.

- **Markers** – The way of expressing and making boundaries visible, is by setting *markers*. In the physical world, a marker would be the 'Keep Out!' sign placed in one's garden, informing other people that this is a private space where entering is not permitted. In digital space, it could be the log-in screens for accessing a personal computer or it could be the 'private' tag put on a folder.
- **Bridge** – The *bridge* is the fourth component of a DT. It differs from the other components in the sense that it is not a component per se, but provides the link between the physical and digital or virtual world; for example, a bridge can be an RFID tag which contains a link to information about the object that embeds it, thus providing a link between a physical entity (object) and its virtual history and thus 'bridging' the physical and the digital world. As the boundaries between these two worlds blur with the development of new technologies in a future AmI environment, the concept of the bridge will become increasingly important in relation to the identification of the personal data-space and the drawing of the DT boundaries.

Furthermore, as a special case and example of DT, IPTS has developed the concept of 'Virtual Residence' (VR), which basically projects the concept of a protected 'residence' in the on-line, digital world. This protection could be either legal or in the form of social norms and 'netiquette'. It relates to the individuals' lives and the personal data stored at home, which at times need to be remotely accessible from the digital world. VR is also an attempt to address the need for more privacy-enhancing initiatives, at least in the 'home environment' which constitutes a first clear example of territory (physical and digital) that may require regulatory protection. VR is an attempt to identify alternative legislation to protect data of a personal nature, exactly as it is protected in our physical homes now. VR is a DT, made up by the integrated DTs of the 'home' residents who take turns in managing the 'shared' data, since in many cases, more than one person use the same physical infrastructures. VR could become the first DT application area, since current applications put additional pressure on taking relevant action, and the issues posed are perceived as easier to address.

If we look at the concept of AmL as developed above, and connect it with IPTS' concept of digital territories and virtual residence, we can recognise many ways in which this conceptualisation of territory in the digital space provides an interesting example for AmL:

- the traditional concept of territory, part of the physical space, is transposed to the digital space;
- the concept of DT acknowledges the need for boundary creation and maintenance as central to privacy, and it aims to empower people to achieve this;
- the concept of DT acknowledges the blurring of private and public space in the digital space, allowing a more contextual approach to privacy (like virtual residence);
- if the concept of DT is made operational by translating it into digital code, it can be used as an example of how to inscribe values or (legal) norms into the architecture of AmI.

## 3.6 Summary of the conceptual exploration

In this chapter, we have explored the concept of Ambient Law. For a start we have discriminated between different conceptions of the relationship between law and technology, favouring a conception that acknowledges that technology is neither good nor bad, but never neutral (section 3.1). We have developed the idea that moral values and legal norms can be inscribed into a technology and argued that as far as this is the case, technological design should be a concern of the legislator, bringing the consequences of such design within the reach of democratic procedure and the rule of law (section 3.4 and 3.5.1). Having discussed that the distinctive features of modern law depend on the fact that its values and norms have been inscribed in the written and printed script (section 3.2), we have argued that for law to remain both legitimate and effective, it will need rearticulation in the emerging architecture of AmI. To provide some first examples of what Ambient Law could imply, we have discussed the concepts of 'contextual integrity' and 'digital territory' (sections 3.5.2 and 3.5.3). To the extent that these concepts can be made operational in digital code and integrated in the legal framework, they will provide a more effective and legitimate type of law, coined Ambient Law in FIDIS deliverables 7.3 and 7.7.

# 4 Assessment of the existing legal framework: overview, effectiveness and lacunae

## 4.1 Introduction

Ambient Intelligence has the potential to overcome many insufficiencies of current information systems. However, it also entails serious threats to individuals and society. Ambient Intelligence promises to offer previously inconceivable levels of support for human activities by technology working imperceptibly in the background. This potentially implies ubiquitous observation and exposure of personal behaviour and habits, preferences and aversions, political affinity and emotional status. Compared to the current situation, the Ambient Intelligence vision implies a tremendous increase in the amount, quality, and accuracy of data generated and collected.[14] As a result, AmI raises questions on the legal safeguards and protection of constitutional values for citizens.

In this chapter, we will make an assessment of the existing European legal framework relevant to AmI, focusing on privacy and data protection. We will also give an analysis of the enforceability as well as the effectiveness and lacunae of the current legislation in relation to an AmI environment.

## 4.2 Overview of the existing privacy and data protection legal framework

The right to privacy is considered a core value of a democratic society. It is recognised as a fundamental right in all major international treaties[15] and agreements on human rights and in the constitutions of several countries,[16] either explicitly or implicitly. In Europe, the fundamental right to respect for privacy is recognised, among others, in Article 8 of the European Convention of Human Rights and Fundamental Freedoms (ECHR),[17] which states that everyone has the right to respect for his private and family life, his home and his correspondence.

With the evolution of technology, it became clear that the mere recognition of the right to privacy was not sufficient to safeguard the privacy with regard to the processing of personal data. Basic principles of data protection were developed and spelled out in international legal data-protection texts produced by institutions such as the Organization for Economic Cooperation and Development (OECD), the Council of Europe (Treaty 108), and the European Union (Directive 95/46/EC). The EU has also included the right to private and family life as well as right to protection of personal data in Articles 7 and 8, respectively, of the European Charter of Fundamental Rights.

[14] J. Cas, Privacy in Pervasive Computing environments – A contradiction in terms?, *IEEE Technology and Society Magazine*, Spring 2005, 25.

[15] Overview of the international instruments in the field of data protection: http://europa.eu.int/comm/internal_market/privacy/instrument_en.htm.

[16] Overview of national legislation in over 50 countries: "An International Survey of Privacy Laws and Developments", Electronic Privacy Information Centre and Privacy International, http://www.privacyinternational.org/survey ; See also: http://www.epic.org.

[17] European Convention for the Protection of human rights and fundamental freedoms, Council of Europe, Rome, 1950, http://conventions.coe.int/; See also article 7 of the Charter of Fundamental Rights of the European Union, O.J. C 364/1, 18.12.2000.

Directive 95/46/EC reconciles the need for a free flow of personal data between the Member States with the need for protection of fundamental rights and freedoms of individuals, notably the right to privacy with regard to such data. The challenges for data-protection law in relation to Ambient Intelligence concern mainly the reconciliation of the principles of data-protection law with the concept of AmI. This challenge emerges because important elements of AmI as well as its supporting technologies show that AmI systems need large amounts of personal data and, in most cases, profiles to work with. In order to provide people with customised information (enhanced goods and services), AmI needs to have personal information.[18] The aforementioned data-protection principles are twofold. On the one hand, there exist obligations on those who are responsible for personal data and, on the other hand, certain rights are conferred to the individuals whose data are collected or processed.

Directive 2002/58/EC – commonly referred to as the Directive on privacy and electronic communications or simply the ePrivacy Directive – specifies and complements the principles of the general Directive into specific rules for the electronic-communications sector.[19] Its provisions apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Community.[20] Whereas Directive 95/46/EC only offers protection to natural persons, the ePrivacy Directive does not only protect rights and fundamental freedoms of natural persons, but also the legitimate interests of legal persons. This directive regulates issues such as confidentiality of communications, the status of traffic data, itemized billing and location based services, and also direct marketing and spam.

The Data Retention Directive[21] applies to providers of publicly available electronic-communications services or of public e-communications networks. The directive aims at harmonising the obligations of these providers with regard to the retention of traffic and location data, as well as the data necessary to identify subscribers or registered users, to ensure that these data are available for law-enforcement purposes. Information to be retained is the information relating to the source and destination of a communication, the date, time, and duration of a communication, its type, the communication device, as well as the data necessary to identify the location of mobile communication equipment. These data shall be retained for a minimum of 6 months and for a maximum of 24 months by the providers. Member States should have implemented the directive into national law by the 15th of September 2007. For data relating to Internet access, Internet telephony and Internet e-mail, the application of the directive can be postponed till the 15th of March 2009.

[18] M. Friedwald, E. Vildjiounaite and D. Wright, SWAMI: The brave new world of ambient intelligence: a state-of-the-art review, January 2006, 140.

[19] Directive 2002/58/EC of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication), O.J. L 201/37, 31 July 2002, replacing Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector, O.J. L 53, 14 January 1998.

[20] Article 3(1) Directive 2002/58 EC.

[21] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.l J. L105, 15 March 2006, p. 54.

## 4.3 Analysis of the legal framework

### 4.3.1 Data Protection Directive

#### 4.3.1.1 Applicability

When we have a look at the different scenarios, it is clear that Ambient Intelligence is impossible without the processing of personal data. But what exactly is meant by personal data? There seems to be some uncertainty and some difference of opinion regarding this concept, which may affect the proper applicability of the existing data-protection framework in different contexts. That is the reason why the Article 29 Working Party has recently published an opinion on the concept of personal data.[22]

In the Data Protection Directive, personal data are defined as

> any information relating to an identified or identifiable natural person. 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.

There are some exemptions to the obligations regarding processing of personal data. Apart from exemptions foreseen in community law, the exemptions under Article 3 take into account the way of processing (processing in manual non-structured form is exempted). The processing of personal data that is carried out by a natural person in the exercise of activities which are exclusively personal or domestic is also excluded from the Directive. It is not clear whether the directive applies when all data are stored and mined within the context of the home, when the processing is done by intelligent agents (e.g., in domotics applications).

The questions remain what is "any information relating to an identified or identifiable person" and what is an "identifiable person". Information is a very broad term. Any sort of statement about a person is personal data, although not necessarily true or proven. The concept of personal data includes information available in whatever form. It can be a sound, a smell, or an image.[23] Images of individuals captured by a video surveillance system can be personal data to the extent that the individuals are recognisable.

In general terms, information can be considered to "relate" to an individual when it is about that individual.[24] It is not always clear whether certain information relates to an individual. In some situations, the information conveyed by the data concerns objects rather than individuals. Those objects usually belong to someone or may be the subject of particular influence by or upon individuals, or they may be physically or geographically close to individuals. It is then only indirectly that the information can be considered to relate to those individuals. The Working Party also pointed to the fact that the same piece of information may relate to different individuals at the same time, depending on what element is present with regard to each one.

A person is identified firstly when the information is sufficient to immediately make clear who the person is. Name and fist name or the National Registry Number can be considered as data that directly identify a person. Secondly, a natural person is also identifiable when, although the person has not been identified yet, it is possible to identify him. According to

[22] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[23] J. Dumortier, "Privacy en gegevensbescherming", *Vlaamse Jurist Vandaag*, 1993, 6.

[24] loc.cit. n.22, 9.

Recital 26 of the Directive, when determining whether a person is identifiable or not, *"account should be taken of all means likely reasonably to be used either by the controller or by any other person to identify the said person"*. This means that a mere hypothetical possibility to single out the individual is not enough to consider the person identifiable, but a realistic possibility is sufficient.

The notion of identifiability is going to be a crucial one in the field of emerging technologies and AmI environments. The possibilities to link objects and natural persons that allow the profiling of the latter and enable their tracking and tracing will be multiplied. How broadly shall the term identifiability be defined? Is the civil identity of a person necessary in order for him to be identifiable, or would it be enough to be able to declare with a high certainty that it is the same person we refer to in different contexts, e.g., a returning customer of a supermarket that can be "identified" via the RFID tag of his watch? Unfortunately, the Opinion of the Working Party did not enlighten such unclear cases that are already a reality in the field of RFID technology and that are going to be exponentially multiplied in an AmI environment.

And while every developer of AmI technologies and new applications is calling for a clarification of the term personal data, the answer provided by the Article 29 Working Party seems rather too relative to provide legal certainty in the present situation. The choice between a purpose based or a contextualised approach is already been in the core of legal debate especially with regard to sensitive personal data.[25] The Working Party in its Opinion combines both approaches, meaning that whether the processing of particular data concerns personal data depend on both the purpose and the context, while even allowing the same data to count as 'personal data' with regard to one data controller while not counting as 'personal data' with regard to another. However, as AmI produces highly contextualised knowledge and information, whereas purposes may become clear only long after the data have been recorded, the approach of the Working Party does make sense. The point is that written law cannot provide any kind of real time legal certainty in the case of such a casuistic application. As discussed in section 3.5.2 the concept of contextual integrity may provide new impetus to the protection of personal autonomy and informational self-determination in an AmI environment, but this would require practical, technological operability of the concept, as advocated by the vision of AmL

The Working Party makes clear that the technological state of the art at the time of the processing, as well as the future technological possibilities during the period for which the data will be processed, have to be considered. Identification may not be possible today with all reasonable means in use today. If the data are intended to be stored for a month, identification may not be anticipated to be possible during the lifetime of the information, and they should not be considered as personal data. However, if they are intended to be kept for 10 years, the controller should consider the possibility of identification that may occur after 9 years and which may make them personal data at that moment. Since technology is developing with great speed, in many cases it will not be possible for the controller to "guess" the means that might be used within some years, let alone after 10 or more years. Especially in AmI environments, where more and more technologies are interlinked, it is likely that new possibilities for identifying people will emerge in due time, and hence, storing data for a period of several years involves a considerable chance for future identification of natural

[25] See *inter alia:* R. Wong, Data Protection Online: Alternative Approaches to Sensitive Data?, *Journal of International Commercial Law and Technology,* Vol. 2, No. 1, 2007.

persons involved. Should this, however, imply that AmI data processing should already conform to the data-protection principles, i.e., a "just in case" applicability of the data-protection legislation?

One relevant factor for assessing "*all the means likely reasonably to be used*" to identify the persons will in fact be the purpose of the data controller in the data processing. In cases where the purpose implies the identification of individuals, it can be assumed that the controller or any other person involved will have the means "likely reasonably to be used" to identify the data subject.[26] This can have important implications in an AmI environment. For example in the context of video surveillance, actual identification will only take place when certain conditions are fulfilled, but because this identification is the purpose of the video surveillance, the whole application will have to be considered as processing of personal data.

There appears to be a division among Member States on whether or not to use a relative approach to the concept of personal data, in the sense that data are considered personal only for someone who can link the data to an identified individual. The laws in some Member States make clear that for instance encoded or pseudonymised data are 'personal' for someone who has access to both the data and the decoding key, but are not personal for someone without access to the key. The Austrian law refers to such data as 'indirectly identifiable data', while other laws add definitions of pseudonymised data, like the German law. The UK law considers only "*data relating to a living individual who can be identified from those data or (…) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller*" as personal data.[27] In other Member States, like Belgium, in principle all data that *can* be linked to an individual are regarded as 'personal', even if the data are processed by someone who cannot make that link. The laws in several other Member States are ambiguous in this respect. Usually, the data-protection authorities tend to agree with the Belgian approach, but they are willing to be flexible with regard to the processing of non-immediately identifiable data. In the case of such processing, whether the laws apply depends on the probability of the data subject being identified, with the nature of the data taken into account. From this, it follows that diverging use is made of recital 26 of the Directive: some emphasise the term 'likely reasonably to be used', and others rather rely on the expression 'to be used either by the controller *or by any other person*'.

The opinion of the Working Party also addressed the issue of pseudonymised data. It made clear that retraceably pseudonymised data may be considered as information on individuals who are *indirectly identifiable*. The use of a reversible pseudonym means that it is possible to trace back to the individual, so that his identity can be discovered, but only under predefined circumstances. In that case, data protection rules apply, but the risks at stake for the individuals with regard to the processing of such indirectly identifiable information will most often be low. That is why the Working Party suggests that these rules can justifiably be more flexibly applied than in cases where information on directly identifiable individuals is processed. With regard to key-coded data in statistical and pharmaceutical research, the explanation of the Working Party is somewhat confusing. However, it seems to come down to the view that if all technical and organisational measures have been taken to assure that the identification of the data subject is not expected or supposed to take place under any circumstance, the Data Protection Directive is not applicable. The Working Party does not

[26] loc.cit. n. 22, 16.

[27] Analysis and impact study on the implementation of the Directive EC 95/46 in the Member States, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

want to go as far as the Belgian legislator did, stating that when data somehow *can* be linked to an individual, they are regarded as 'personal' even if the data are processed by someone who cannot make that link.

The Working Party states that the determination whether information can be considered as anonymous or not depends on the circumstances. A case-by-case analysis should be carried out with particular reference to the extent that the means are likely reasonably to be used for identification as described in Recital 26 of the Directive. This statement, however, does not make clear what has to be done when anonymous data are collected, but whether – as is often the case with profiling technologies – afterwards the combination of several anonymous data leads to identification. Such a vague approach can have crucial impact on the processing of biometric data, which are in principle used in a pseudonymous or even in an anonymous way. When the biometric data are backtracked to the individual they are linked to, the consequences for the latter can be immense, given that they can be used as the source to reveal a lot of information about him. In cases whereas it can not be guaranteed that backtracking to the individual the data refer to is technically ruled out, the biometric data shall be adequately protected.

In an AmI environment, biometric data will often be used. These data may be defined as biological properties, physiological characteristics, behavioural traits or repeatable actions where those features or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain likelihood. Typical examples of such biometric data are fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns and some deeply ingrained skill or other behavioural characteristic (such as handwritten signature, keystroke patterns, gait, or speech).[28] A wide and unrestricted use of biometrics raises concerns with regard to the protection of the privacy of individuals.[29] Though biometric data is not by definition "information relating to a natural person", in the context of biometrical identification, the person is generally identifiable, as the biometric data are usually used for identification or authentication of the data subject. It follows, in the Working Party's opinion, that biometric data fall under the definition of personal data within the meaning of the Directive. Consequently, their processing must take place in accordance with the principles and procedures stipulated in the Directive.

#### 4.3.1.2 Effectiveness and adequacy

This section will not be a full analysis of the Data Protection Directive; instead, the main problems that can arise when the Directive should be applied to an AmI environment will be presented.

***Consent***

Personal data may only be processed in a legitimate way if the data subject has unambiguously given his consent. If there is no unambiguous consent, it is allowed if the processing is necessary for:

1. the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or

[28] loc.cit n.22, 8

[29] Cf. FIDIS Delilverable D3.2: A study on PKI and biometrics and D3.6: Study on ID documents, regarding the use of biometrics in identification documents.

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 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 the purposes of fundamental rights and freedoms of the data subject.[30]

Without prejudice to any other possibilities,[31] the processing of personal data in an AmI environment may need to be justified by the consent of the data subject, which can be defined as "any freely given, specific and informed indication of his wishes".[32]

The requirement of informed consent presents particularities in AmI. Studies have shown today that users of AmI environments face basic difficulties not only in realising the involvement of devices, which they can not see or feel in most of the cases, but also in understanding their functionality and consequently their use, as well as the actual collection of their data revealing personal information about their preferences, location etc.[33] As Beckwirth[34] clearly states "reliable, inconspicuous sensing of personal information is problematic because users do not always understand the extent or methods of data collection and thus can not adequately evaluate privacy issues". In AmI environments the vast majority of decisions are taken by automated procedures and are based largely on automated profiling, an issue that is dealt with in detail below under 4.3.1.2 – non discrimination.

The consent in AmI is not given by signing a contract, as it is usually the case in the conventional transactions that entail processing of personal data. It can be given by pressing a button or clicking an option, but the issue becomes much more complicated when no tactile interface is available and thus the expression of consent in such a way is physically impossible.[35] Can the processing of personal data be based on one of the other grounds mentioned in Article 7 of the data protection directive and could then the consent of the person who is entering the AmI environment be considered as redundant? Some AmI applications are designed to assist elderly people, for instance, and in this case it can be sustained that the processing of the personal data is necessary in order to protect the vital interests of the data subject and therefore the consent of the latter is not needed.

Furthermore processing of personal data can be justified under the ground that the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject […]".[36] For the application of this ground, the local law shall be examined in detail in order to determine its applicability and define what qualifies as legitimate interest, as in this case a

[30] Article 7 of Directive 95/46/EC.

[31] In certain circumstances there might be a legitimate interest of the data controller and is some cases the processing of personal data can be necessary for the vital interest of the data subject. Sometimes it will be necessary for the fulfilment of a contract.

[32] Article 2(h) of Directive 95/46/EC.

[33] R. Beckwith, Designing for Ubiquity: The Perception of Privacy, *Pervasive computing* (April-June 2003), pp. 40-46

[34] loc.cit. n. 33

[35] M. Langheinrich, Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, *Proc. 3rd. Int'l Conf. Ubquitous Computing 2001*, Springer, p. 285.

[36] Article 7 (f) data protection directive.

balance between the interests of the data subject and the controller has to be found.[37] It is interesting to question whether the pursuit, promotion and marketing of legitimate businesses can be considered as legitimate interest.[38]

The existence of multiple devices in a system and the necessity of consenting to the collection and processing of personal data from all of them can become cumbersome for the user. Profiles stored in a personal assistant, such as in the case of David in scenario II, who uses a family preferences agent, coupled to selectable identities, could provide situation-specific consent or dissent.[39] Evidently consent may not always be necessary, because the grounds referred to above apply. For example, data can be collected to warn passers-by taller than 2.15 that a small passage is just around the corner (ground d or f, art. 7), while one can expect service providers to conclude contracts with consumers for long term and wide-ranging services (ground b, article 7). However, one could question to what extent the consent given at the time of concluding such contracts can be considered a free consent. AmI technologies will immensely enhance the quantitative and qualitative possibilities of monitoring and extend it to areas that are currently out of reach of permanent and unobtrusive surveillance.[40] Customers will most probably not be aware of the scope and impact of the data that will be collected and the types of profiles that can be inferred from them. When the individuals wish to enjoy the benefits of such AmI technologies, how can they be informed about the constant collection and processing of their personal data? How can the traditional notion of consent be adjusted to the developing word of AmI technologies? There is almost no possibility to escape the supervision infrastructure for those parts of the population who do not want to be permanently observed. Can a "consent free of doubts" to something that is practically unavoidable count as a valid part of individual or collective agreement at all? And, even if consent is not necessary, the grounds for legitimate processing of personal data will continuously shift, depending on the context, requiring constant alertness of both the user and the provider. This would render the whole concept of unobtrusive proactive anticipation invalid. AmL could provide some answers here, meaning for instance that one carries a PDA that seamlessly negotiates consent while applying mandatory parts of the directive (checking relevant grounds for legitimate collection of data).

### *Purpose specification and proportionality*

Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.[41]

The aim of AmI technologies is not to serve single purposes, but to support the users in a variety of more or less foreseeable situations. The purpose of data collection lies entirely in the accumulation of as much information about individual behaviour patterns and preferences as possible. The context in which this knowledge is going to be applied remains necessarily unclear at the time of collecting the data.[42]

[37] Ch. Kuner, *European Data Protection Law*, Oxford University Press, 2nd edition 2007, par. 2.35.

[38] R. Jay & A. Hamilton, *Data protection – Law and Practice*, London, Sweet & Maxwell, 2003, par. 6-11.

[39] loc.cit. n. 14., 30.

[40] loc.cit. n. 14, 29.

[41] Article 6 (b) Directive 95/46/EC.

[42] loc.cit. n.14 29.

It is difficult to comply with the rule that further processing of personal data must be compatible with the purpose specified at the time of data collection, if there is no initial purpose. And even if there is one, collected data may serve for other applications or purposes that are discovered only later. The creation and use of databases may often create additional benefits, for example in the case of profiling.[43] Apart from numerous technical problems, a limitation of the transfer and use of data would entail that every attempt to enforce parts of this principle implies curtailing the benefit and the usability of Ambient Intelligence infrastructures. Cas points to the fact that benefits will be limited, because an invariable assignment of data to applications limits the adaptability and learning abilities of the system.[44]

It also has to be kept in mind that the purpose-specification principle restricts the possibility to link different forms of processing and databases for profiling objectives. The purpose-specification principle is definitely at odds with the logics of interoperability and availability of personal data.[45] When we look at the different scenarios, it becomes clear that profiling is crucial in an AmI environment, for example, for the dating service in scenario I. The purpose-specification principle makes this difficult, perhaps impossible. In the context of profiling, special consideration also needs to be given to Art. 15 (1) of the Data Protection Directive. This article gives the right to every individual

> 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.

This prohibition seems equally at odds with the logic of adaptive autonomic profiling, as discussed, since most decisions will be taken by machines in a process of machine-to-machine communication.

Personal data must also be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.[46] This is the data-minimisation principle. It is clear that in an AmI environment, the amount but also the quality of data that are collected, will seriously increase, thus infringing the data-minimisation principle. Even if only part of this huge amount of data is stored or analysed, this principle will be fully turned upside down. The whole concept of AmI is data maximisation, i.e., to collect as much information about individuals as possible in order to be able to offer them customised services. Suggestions have been made, instead of focusing on reducing the amount of data collected, to admit that they are indispensable for AmI, and to focus rather on empowering the user with a means to control such processing of personal data.[47] Data protection is a tool for empowering the individual in relation to the collection and processing of personal data, but it should not be turned into an insurmountable obstacle to progress and technological development. The Data Retention Directive, which calls for the retention of a large amount of personal data in order to have them available for law-enforcement purposes, reveals the willingness of the European legislator and the Member States to put the data-minimisation principle aside in certain

[43] Wright D., SWAMI project, Final Report, August 2006. Download http://swami.jrc.es/pages/documents/SWAMID4-final.pdf, 140.

[44] loc.cit. n.14., 30.

[45] P. De Hert, "What are the risks and guarantees need to be put in place in view of interoperability of police databases?" in European Parliament. Directorate-General for Internal Policies of the Union (ed.), *Area of Justice, Freedom & Security, Collection of Standard Briefing Notes by External Experts,* Brussels, Parlement Européen (Ed.), Jan.2006-March 2006.

[46] Article 6 (c) Directive 95/46/EC.

[47] loc.cit. n.43, 136.

circumstances. Whether a similar approach will be followed in AmI in order to allow the full operation of the relevant systems remains to be seen.

### *Transparency*

Transparency is an important principle of the Data Protection Directive. The Directive does not forbid the processing of data,[48] but it does require data processors to inform data subjects with regard to which data are processed, the identity of the one who processes them, and the purpose. For example, when cameras are placed at a workplace, the employers have to be informed about the camera policy. The employer will have to inform the employees about every aspect of the camera surveillance, like the location of the cameras and whether the images will be stored and for how long.

Nowadays, it is already very difficult to know in full detail who collected which data, to which organisations the data were transferred, and for which purposes they were used, despite the data-protection legislation commanding otherwise. But still, users are most of the time aware that they providing personal data when, for example, filling in an online or offline form. This will be totally different in an AmI environment, where users will ever less be an active and conscious source for providing personal data. The desire to provide Ambient Intelligence in an unobtrusive manner requires a framework in which users are permanently observed and their behaviour and actions autonomously interpreted, taking into account location and other contextual information. The results are then fed into a continuous learning process, which will form the basis for autonomous decisions by the AmI system on how and when to use, or to pass on, the collected information. It is clear that the already existing information asymmetry between data subject and data controller will significantly enlarge.[49]

The transparency principle is specified in the right to be informed. In case of collection of data not from the data subject himself, the controller must always provide the data subject with at least:

1. the identity of the controller or his representative, and
2. the purposes of the processing for which the data are intended.

Further information to be provided if necessary to guarantee a fair processing, are

3. the recipients or categories of recipients of the data,
4. whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and
5. the existence of the right of access to and the right to rectify the data concerning him must only be given "in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject".[50]

It is clear that the practical application of this right in an AmI environment will bring along a serious burden for the data controller and for the data subject. Because of the large amounts of

[48] Except in some circumstances, like the transfer of personal data to third countries that do not ensure an adequate level of protection.

[49] loc.cit. n. 14, 27.

[50] Article 11 Directive 95/46/EC.

data to be processed in an AmI world, the help or support by intelligent agents to manage such an information stream seems indispensable.[51]

### *Non-discrimination*

The majority of decisions in AmI are made based on profiles, either individual or group ones. The use of such profiles for making decisions upon services and applications to the users of AmI environments is of dual legal importance. On one hand it is to be examined whether such decisions can be considered as fully automated decision making, thus falling under the provisions of Article 15 of the data protection directive and on the other hand whether such practices infringe existing non discrimination legislation.

Decision making procedures in AmI are mainly automated and are based on profiles of the users of the systems. According to Article 15 of the data protection directive the "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct etc.". As Bygrave has very clearly summarised for Article 15 to apply four conditions have to be satisfied cumulatively:

- "a decision must be made;
- The decision concerned must have legal or otherwise significant effects on the person whom the decision targets;
- The decision must be based solely on automated data processing;
- The data processed must be intended to evaluate certain personal aspects of the person who is targeted by the decision."[52]

Great importance in AmI has the first of the aforementioned conditions, i.e. to what extent a decision is made in an AmI environment. Bygrave suggests a broad interpretation of the term "decision" that does not necessarily entail the involvement of human and therefore the "decisions" made in AmI can be considered as such, and Article 15 applies.[53] By accepting that Article 15 applies in AmI environments the data subject is also granted the right to know the logic involved in the automated processing[54]. However as Beckwith has stated "[i]n the case of embedded sensor technologies, it would be practically impossible to teach anyone the system's full implications".[55] The actual exercise of this right is still to be examined.

The fact that the decisions in AmI are based on profiles has raised the question whether they infringe existing non-discrimination legislation. Article 14 of the European Convention on Human Rights (the 'Convention')[56] and Article 1 of Protocol No. 12 to the Convention ('Protocol No. 12')[57] will serve as the basis. These articles prohibit the discrimination from

[51] loc.cit. n. 43, 137.

[52] L. Bygrave, Automated Profiling – Minding the machine: Article 15 of the EC data protection directive and automated profiling, *CLSR,* Vol. 17 no 1, 2001, p.17.

[53] loc.cit. n. 52, p. 19

[54] Article 12 (a), al. 2 data protection directive

[55] loc.cit. n. 33, 44

[56] Convention for the Protection of Human Rights and Fundamental Freedoms, *European Treaty Series, N° 5,* also available at http://conventions.coe.int/Treaty/en/Treaties/Word/005.doc (last visited on 12 April 2006).

[57] Protocol No.12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, *European Treaty Series, N° 177,* also available at http://conventions.coe.int/Treaty/en/Treaties/html/177.htm. The Protocol

the States towards individuals. This would mean, that "if profiling practices conducted by public bodies representing the state (i.e. the (local) government) would be proven to be discriminatory, these provisions could be invoked by an individual who could require from the government that the discriminatory profiling practice in that specific case is stopped ('vertical effect')".[58] However there are arguments to sustain that these rights can be applied also in private relationships.[59]

The use of specific criteria, such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status, as described in Article 14 ECHR can not be used as ground for discrimination. The wording of Article 14 ECHR "or other status" leaves it open as to what other criteria are considered a discriminatory ground.[60] However the whole nature of AmI is based on a faddish way of discriminating among the users of a system and making decisions based on profiles that are built upon various criteria. Could it be sustained that AmI technologies are violating non-discriminating legislation as they are based on the processing of personal data and the consequent building of profiles?

### 4.3.2 ePrivacy Directive

#### 4.3.2.1 Scope of application

Directive 2002/58/EC applies to the processing of personal data in connection with the provision of publicly available electronic communication services in public communication networks in the Community.[61] An electronic communications service is defined as:

> a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

Briefly put, this covers services that consist in the public conveyance of electronic-communication signals. It can be noted that information-society services are explicitly excluded. This means that the ePrivacy Directive contains obligations for transporters of data and not for content providers. This is important to take into account, as the distinction between an electronic-communications service and an information-society service is not always clear. Recital 10 of Directive 2002/21/EC (Framework Directive) in fact refers to electronic mail as an example of a service which constitutes both an electronic-communications service and an information-society service. It is also important that the ePrivacy Directive only applies to publicly available electronic communication services in public communication networks. In European legislation, there is no definition of what

No. 12 has been opened for signature since 4 November 2000, and came into force on 1 April 2005 after ten ratifications (there are as of 12 April 2006 22 signatory states (without ratification) and 13 ratifications (list available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=177&CM=8&DF=4/12/2006&CL=ENG).

[58] W. Schreurs, M. Hildebrand, E. Kindt & M. Vanfleteren, Chapter 13: Cogitas, ergo sum. The role of data protection law and non-discrimination law in Group profiling in the private sector, in M. Hildebrandt, S. Gutwirth (eds.) *Profiling the European Citizen - Cross-disciplinary perspectives,* Springer 2007.

[59] loc.cit. n. 58

[60] loc.cit. n. 58

[61] Article 3(1) of Directive 2002/58 EC.

'public' exactly means here.[62] So it is not that simple to know exactly when the Directive is applicable. It is clear that when all data are stored and mined within the context of the home and remain within the private network of intelligent agents that are running the house, the ePrivacy Directive will not be applicable. This will be different when an individual makes use of a locator service when visiting New York. With regard to this it has to be said that the Article 29 Working Party has stated that the fact that provisions of the ePrivacy Directive only apply to public services over public communication networks is regrettable, because private networks are gaining in importance in everyday life; the risks increase accordingly, in particular because such networks are becoming more specific (e.g., monitoring employee behaviour by means of traffic data).[63] In this respect it is questionable whether the restriction to 'public' networks and services can or should be upheld in the future.

### 4.3.2.2 The applicability of the ePrivacy directive in AmI

As already described under 4.3.2.1 the crucial point for the applicability of the ePrivacy directive is whether there is processing of personal data in connection with the provision of *publicly* available electronic communication services in *public* communication networks. The ePrivacy directive contains important provisions regarding traffic and location data, mainly Articles 5, 6 and 9[64], that will only apply when the relevant services and networks are *public*. In AmI, however, having a public network or offering a public service is not an intrinsic element of the system. This point however is crucial in deciding upon the applicability of the ePrivacy directive, and especially the application of the provisions regarding Location Based Services.

In an AmI environment Location Based Services can be either public or private services that are offered either in public or private networks. It would sound reasonable that no matter what technology is used for the offering of the service and whether it is public or privacy, the legal framework regulating it shall be the same. However the wording of the ePrivacy directive leaves no doubts that its provisions shall not apply when the service or the network used is not public.

More specifically Article 9 deals with the location based services and states that location data other than traffic data may only be processed if the data are made anonymous, or with the consent of the users or subscribers of the service to the extent and for the duration necessary for the provision of a value-added service. Paragraph 2 of this article states that, even when the user or the subscriber has given his consent, he shall have the possibility to refuse the processing of the data temporarily or permanently at all times. The processing of the location data shall be necessary for the value-added service and shall be limited to the duration necessary to provide this service. So, with regard to location data other than traffic data, unnecessary processing is prohibited, unless the derogation of Article 15 applies to the situation or as far as the Data Retention Directive applies. It is obvious that location-based services play a central role in AmI, as a vast amount of services are offered based on the processing of location information of the user.

An illustrative example from scenario II is the service offered to David via his MyComm device that allows him to find a restaurant close by that will match his taste and preferences.

[62] Cf., FIDIS Deliverable D11.5, in particular section 4.3.3.

[63] Ibid., section 4.7 *et passim*.

[64] Idis, section 4.3.2, where a very clear illustration of the classification of data into personal, traffic and/or location data is available.

The MyComm device is described as "a 5th-generation mobile device with many useful functions and access to location-based services". As such location bases services are accessed by MyComm via the public mobile network, they qualify as value-added services in the sense of Article 9 ePrivacy directive and the special provisions of the directive apply. But let's take a look at the following scenario: Let's assume that MyComm, as a 5th generation mobile device, is equipped with RFID and Bluethooth that also enable the provision of Location Based Services. Although these technologies transmit data in a wireless way, it is not beyond question that they would qualify as using a public communications network and offer a public communications service.[65] Although, even in the latter case, the general provisions of the data protection directive will apply, not leaving the user of the services without any legal protection, the special provisions of the ePrivacy directive may not apply. In this case we would have the paradox that services offered from the same device via the use of different technology will fall under different legal provisions. Was such a result aimed by the European legislator when he was enforcing the ePrivacy directive aiming at a technology neutral piece of legislation?

## 4.4 Conclusion

The analysis of the European legal framework on data protection aimed at illustrating the main principles that apply in an AmI environment and to discuss the *lacunae* in legal protection that can arise. Taking into account the fact that the general Data Protection Directive was adopted in 1995, it can easily be explained why some of the most important principles on which current privacy protection is based contradict the vision of Ambient Intelligence – an AmI world was simply not thought of when the data-protection framework was conceived. However, as has been clearly illustrated, even the provisions of the more recent ePrivacy Directive do not manage to keep up with the technological developments: it is not always easy to determine whether a service is an electronic-communications service or an information-society service in order to identify which legal provisions apply, and there is no clear justification why the specific provisions of the ePrivacy Directive on location-based services only apply when the service is offered via a publicly available electronic communications network and not via a private network.

The data-protection legislation aims at the protection of individuals against the unjustified processing of personal data. The existing legislation imposes quite severe restrictions on the processing of personal data, based mainly on a model where there is a direct – be it on-line or off-line – contact between the controller and the individual in question. This is an outdated paradigm in light of the vision of Ambient Intelligence. Therefore, careful reflection is required on the interaction between the legal obligations in the current legislative framework and the development of new emerging technologies and AmI applications. Neither should be allowed to completely overrule the other.

[65] Ibid, section 4.3.3.

# 5 Assessment of PETs and TETs: overview, effectiveness and lacunae

## 5.1 Introduction

AmI space, as described in FIDIS deliverables 7.3 and 7.7, implies real-time monitoring, proactive computing, and autonomic adaptation of the environment. In traditional AmI scenarios to facilitate this, large centrally available storages of personal data are used, which store any sensor data available and mine them dynamically to support the adaptation of the environment. In most cases, this happens unrecognised and unobserved by the data subject and under the control of one or more third parties. In these scenarios, data maximisation is an important quality element – the more data (relevant for a proper adaptation) the backend systems will have to mine, the better the quality of the AmI systems can be.

As already outlined by Čas in 2005 (Čas 2005) and analysed in the previous chapter, these scenarios fundamentally run against the principles of data protection, especially reliable legal grounds, the data minimisation principle, the transparency principle, and in many cases the purpose-binding principle as well. Čas argues that as data storage becomes very cheap, there is no economic incentive for deleting data. In contrast he lists a number of examples where data collected and stored for one purpose in the AmI environment well may be used for a different purpose very cost efficient. He concludes that the technical functional principles of AmI together with the economic driving forces will lead to an increasing information asymmetry between data subjects and operators of AmI environments.

One of the curious characteristics of Ambient Law as discussed in chapter 2 is that the seperation between the written law and its enforcement that is a hallmark of modern law can no longer be taken for granted. If legal rules are inscribed or embedded in computer code their inscription may rule out violation of the rules (which is one of the important issues in the design of AmL: safeguarding the contestability of such rules). Over the past years, in the context of AmI, a number of Privacy Enhancing Technologies (PETs) and Transparency Enhancing Technologies (TETs) concepts have been developed or discussed as potential future solutions. They might develop into interesting examples of AmL, in as far as their implementation becomes part of the legislators' ways to enact privacy regulation.[66] Taking the definitions used in FIDIS deliverable D7.7, we have:

**PETs** (privacy enhancing technologies) are defined as "a coherent system of ICT measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system." (Borking 1996, translation taken from Borking, Raab 2001).

**TETs** (transparency enhancing technologies) anticipate profiles that may be applied to a particular data subject. This concerns personalised profiles as well as distributive or non-distributive group profiles, possibly constructed out of anonymous data. The point would be to have some idea of the selection mechanisms (application of profiles) that may be applied, allowing a person adequate anticipation. To be able to achieve this, the data subject needs

[66] In fact, PETs are already used as a way to implement the existing written law, which may lead to different levels of implementation of the same law. Getting the legislator involved in stipulating that its democratically legitimised rules are inscribed in all the relevant technologies would provide a more effective and a more general application of the law.

access – in addition to his own personal data and a profiling / reporting tool – to additional external data sources, allowing some insight in the activities of the data controller. Based on this additional information the data subject could perform a kind of counterprofiling.

In contrast to PETs, where the principle of data minimisation is a key element, TETs take a very data-intensive environment into consideration where the data collection is not necessarily related to the individual as such. The more is known about the actual (or even possible) data processing and can be used by TETs to anticipate profiles, the more accurate these results can be. Thus, TETs are based rather on data maximisation which does not only include all data released (if available), but also information on methods and profiling algorithms as well as data from other sources utilised by data controllers, possibly also information on security breaches if this leads to other findings. These data could also be parameterised by probabilities if it is uncertain information.

We see already from the quoted definitions that the terms are related because both PETs and TETs can help data subjects to maintain their privacy. Transparency as such – in the meaning of "clear visibility" – is an underlying principle both for PETs and for TETs:

- Transparency of data processing usually is a prerequisite for effective protection of privacy; however, it is not a sufficient condition: mere transparency does not guarantee privacy compliance.
- Transparency of the data subject's personal data should be provided by PETs for the data subject itself to increase its knowledge on data processing and empower it to choose on desired and undesired processing of personal data – this is the same with TETs.

There is an important difference, however: PETs should protect the data subject's personally identifiable information against unauthorised access, e.g., by using confidentiality mechanisms. These confidentiality mechanisms can be on the content level (e.g., encryption, access control) or on the communication network level (e.g., anonymising/pseudonymising techniques or other mechanisms to prevent linkability). These mechanisms clearly do not belong to the transparency techniques, but rather to the contrary: the opacity techniques.

According to the definition of TETs, the data subject is in the focus, too, to get information on the potential profiles about itself. It is debatable how much "counterprofiling" is possible in reality and how it can be balanced with other potential interests, e.g., from other data subjects: To really mimic the profiling which is done by a data controller (or which could be done by a hacker), i.e., to perform an effective counterprofiling, it may be necessary to make use of personal data of other data subjects as well. E.g., if a data subject has statistical twins whose detailed information is known, this knowledge may be extrapolated to apply to the data subject itself which originally has not provided that many data. Even in the case of anonymised instead of personally identifiable data, the profiles may contain so much information that the possibility to re-establishing the links to the related data subject could not be eliminated (cf. Hansen et al. 2007). Thus, there may be TETs which perform – with good intent to mimic the original (or potential) profiling done by a data controller – privacy-invasive processes.

A pared-down interpretation of "counterprofiling" would limit its scope to information on the logic of data processing, possibly additionally taking into account data sources which are not privacy-invasive.[67]

This chapter first elaborates on traditional PETs in both its opacity and transparency properties and then analyses potential technological concepts for TETs. In both subsections the current state of the art in development, their effectiveness, and lacunae are described.

## 5.2 Overview of AmI-relevant PETs

Traditionally, PETs are mostly categorised by the technologies used, the area of application, or standardisation efforts. Examples are the classes of Identity Management Systems (IMS) introduced by Bauer, Meints, and Hansen (2005: 19ff). In the context of AmI (and thus also AmL), however, relevant PETs can also be categorised using more abstract criteria, e.g., whether they primarily support:

- transparency for the data subject on all relevant data processing concerning him, as far as his personal data, are concerned or
- opacity for potential observers or data-processing entities of data or actions concerning the data subject.

In the context of AmI, the most relevant PETs are the following.

- Opacity-enhancing functions and tools concerning data and actions of the data subject, in particular tools and mechanisms limiting the linkability of data to a person,[68] such as:
    - use of different pseudonyms per context, possibly transferable to other users;
    - use of Privacy Preserving Data Mining (PPDM) techniques;
    - disabling or management of sensor functionality as desired by the data subject.
- Transparency-enhancing functions and tools for the data subject, such as:
    - protocols to visualise and exchange privacy policies;
    - history management;
    - online functions for users to exercise their right to access their personal data according to the data protection legislation which enables the data subject to see what the data controller knows about itself, i.e., enhance transparency, and to take further actions if necessary (cf. Hansen 2007);
    - provision of ad-hoc additional information (e.g., as audio-visual tags or asynchronously via separate channels such as websites, RSS feeds etc.) to data subjects concerning the environment they are in or concerning the reputation of data-processing entities involved.
- Supporting Technologies:

[67] The definition and concepts of TETs will be further elaborated in FIDIS deliverable D7.12.

[68] This comprises both limiting the linkability of data directly to a person and, more indirectly, limiting the possibilities for observed data of a person to be aggregated to pseudonymous profiles, so that they do not give enough information to yield the link to the person behind that profile.

  - Cryptography as an important instrument for access control and thus confidentiality (support for opacity). Cryptography is not elaborated further in this chapter.
  - Digital Rights Management (DRM) for personal data, supported by additional technologies such as Trusted Computing (TC, see section 5.2.3 for further explanation of DRM and TC).

- Combined approaches:
  - Concepts to shift control in AmI environments to the user, e.g., supported by a personal digital assistant (user-controlled identity management).

These tools will be elaborated in the next sections.

### 5.2.1 Opacity-enhancing functions and tools

Opacity-enhancing functions and tools aim at limiting the linkability between personal data and the data subject. This can be achieved in many different ways. Commonly used methods are:

- use of transaction-specific or context-specific pseudonyms, together with additional organisational measures to prevent linkability across borders of transactions or communicational contexts. Technically, this can be supported by credential systems such as “Credentica” and “Idemix” or sector-specific identifiers as used by the Austrian citizen card;[69]
- use of Privacy Preserving Data Mining (PPDM) techniques and methods. Most relevant in this context are the modification of attributes (basic data) and the use of special privacy-preserving data-mining algorithms to allow data or rule hiding (Verykios et al. 2004).

The use of context-specific pseudonyms is nowadays mature from a technical perspective. However, the AmI approach does not seem to provide relevant economic incentives for their use from the perspective of service providers. The use of pseudonyms and additional organisational measures increases the complexity of AmI systems, while at the same time limiting the amount of data available for processing, and thus potentially limiting the quality of AmI services.

Privacy Preserving Data Mining has been an area of research already since 1991.[70] PPDM is used to support the privacy of data subjects or organisations taking part in mining of distributed data. The latter application is not relevant in this context.

Though PPDM has been used especially in the health sector,[71] so far, PPDM is not widely used. From the perspective of Oliveira and Zaïane (2004), the most relevant hindering factors are (a) very specific areas of application for many methods, (b) lack of integration in data-mining solutions, and (c) difficulties to measure the reached quality of the mined results and privacy protection reached along the way.

[69] Digital credential systems have been elaborated in FIDIS deliverable D3.1, and sector-specific identifiers in the context of the Austrian Citizens Card in FIDIS deliverable D3.6.

[70] See for example overview up to 2004 at http://www.cs.ualberta.ca/%7Eoliveira/psdm/workshop.html.

[71] See for example http://www.lustat.ch/ms_Datenschutzkonzept_2001.pdf and, more recently, http://e-hrc.net/media/ExtHealthNetworksMuscle02Feb2005.htm.

The understanding of PPDM seems to be largely technically focused (Meints, Möller 2007). As a result, PPDM is not able to cover all relevant data-protection principles, e.g., as stated in the OECD Guidelines (Oliveira, Zaïane 2004). Far better results to preserve privacy can be achieved when PPDM is used in the context of good-practice standards for data mining, such as CRISP-DM[72] or Knowledge Discovery in Databases (KDD) in case compliance with data protection is understood as part of the business targets (Meints, Möller 2007).

In the context of RFID, selective and non-selective disabling of sensors has been discussed. Juels, Rivest and Szydlo (2003) have developed so-called blocker tags that perform a denial–of-service attack on any reader in range by simulating a large number of different tags. Based on the same technical functions used for the blocker tag, Rieback, Crispo and Tanenbaum (2005) have developed a device for RFID privacy management. This device allows selective blocking of single RFID tags in range. Blocker tags and the "privacy manager" can be used with certain types of RFID tags only; the remaining types of passive RFID and certain biometrics do not support any kind of user-controlled identity management yet (Bizer et al. 2006, 314).

Spoofing of RFID readers using manipulated or copied RFID tags also has been discussed as an approach to enhance the privacy of data subjects (e.g., by Thompson et al. 2006). This approach also has been used in the scenario II (section 2.2, scene 2).

## 5.2.2 Transparency-enhancing functions and tools

### 5.2.2.1 Automated privacy policies

Traditionally, to support transparency of data processing, privacy policies are used internationally. In the late 1990s, first attempts were made to formalise privacy policies with the aim to make them machine readable and to support automated processing. As a first result, the Platform for Privacy Preference (P3P) protocol was standardised by the W3 Consortium (W3C) in 2002 in a first version (V1.0).[73] Based on P3P, A P3P Preference Exchange Language (APPEL) was planned, but standardisation is dormant.[74] Instead of APPEL, together with P3P, also XPref can be used to exchange privacy preferences (e.g., Kolari et al. 2005).

P3P together with XPref supports expressing privacy policies by operators of web sites in a formalised language. These privacy policies can be compared with privacy preferences of the users entered in their browser or tools integrated in browsers (plug-ins). These tools support the comparison of privacy policies published by the operators of web sites and preferences entered by users, and they will inform users in cases of discrepancies.

Other relevant approaches are the Enterprise Privacy Authorization Language (EPAL, suggested by IBM in 2003 based on XML).[75] An overview of languages for formulating, comparing, and negotiating privacy preferences will be given in the FIDIS deliverable D3.8.

These approaches can be understood as an early version of machine to machine (M2M) communication between a client (in this case a browser and based on personal preferences)

[72] See http://www.crisp-dm.org.

[73] See http://www.w3.org/TR/P3P/.

[74] See http://www.w3.org/TR/P3P-preferences/.

[75] The current specifications (V 1.2) are available via http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/.

and a server offering a centralised service (in this case a web-server). Human Machine Interfacing (HMI) has been adapted to deal with the results of the previous M2M communication. This kind of M2M communication and HMI can be understood as predecessors of the communication of David's MyComm-device at the hotel (section 2.2, scene 1).

#### 5.2.2.2 History management

An overview of the state of the art in history management and recent research is given by Meints (2006). History management was introduced by Hansen et al. (2003) as an important identity-management function of user-controlled IMS (also called type 3 IMS). The most important prerequisites for the applicability of history management is that the data subject actively discloses his personal data with a device that allows for logging of transferred data and later analysis.

Typically, history management so far is used in the context of web services accessed via a personal computer. Brückner (2003) developed the so-called data journal (later called IJournal), the first usable implementation of history management for Mozilla-based browsers. The IJournal is further developed as part of MozPETs (Mozilla PETs, Brückner, Voss 2005).

This concept was significantly improved in the context of the project PRIME – Privacy and Identity Management for Europe (PRIME 2007). Basing themselves on the main architecture of the PRIME prototypes as well as on first descriptions of related TETs in FIDIS deliverable 14.2, Hansen et al. (2007) describe methods to increase transparency for users on privacy-relevant data processing, so that they can maintain the control over their private sphere. These transparency tools are particularly valuable because they inform the user via one integrated interface of a user-controlled identity-management prototype. Basically, five transparency tools are fully or partially implemented in PRIME prototypes:

- log functionality on the user's side: the so-called Data Track (cf. FIDIS deliverable 14.2),
- warn functions for signalling possible mismatches with the user's preferences,
- tutorials and demo tools,
- a security feed to report and react to vulnerabilities, and
- on-line help functions which enable users to exercise their rights and to keep control over personal data which they have released.

The PRIME prototypes do not address the AmI world but rather the world of Internet and mobile communication. However, the prototypes' underlying concept is valid for AmI, too, as comprehensive information on data processing as well as on potential or actual risks has to be provided if users should be in control over their private sphere.

### 5.2.3 Supporting technologies

Supporting technologies are mainly used in the context of combined approaches (see section 5.2.4).

#### 5.2.3.1 Digital Rights Management

In the context of transparency and opacity tools, Digital Rights Management (DRM) and Trusted Computing (TC) have been discussed as relevant supporting technologies. Depending on the implementation, both technologies can support transparency as well as opacity, and this both from the perspective of the data subject and from the perspective of an observer or data controller.

The term DRM indicates methods that help copyright holders to control the access to digital content (Grimm et al. 2005: 16). Typical technical methods used in the context of DRM are:

- access control for digital data (such as passwords for subscribers of online journals);
- copying-protection mechanisms.

From a technical perspective, today's DRM solutions have mostly proved to be ineffective (Bizer et al. 2006: 132), as they can be circumvented, e.g., via analogue data channels (analogue audio tracks or paper printouts of (digital) documents). Analogue data can be re-digitalised, e.g. using, audio capturing systems or optical character recognition (OCR)).

Currently new approaches using Trusted Computing to enforce digital rights are areas of research (see e.g., Reid, Caelli 2005).

### 5.2.3.2 Trusted Computing

In terms of supporting technologies, Trusted Computing is an emerging, powerful tool to enforce multilateral legal policies and thus, to support the concept of Ambient Law.

While traditional security technologies can provide adequate security and trustworthiness for one party (in terms of our example scenarios, either for the provider or for the user), providing fair, non-discriminating security and trustworthiness for all relevant parties needs a technology that supports multilateral security. The concept of multilateral security was introduced by Günter Müller et al. (1999) and aim to meet the security needs of all participants.

In a nutshell, Trusted Computing technology provides multilateral security in information processing by providing enhanced components that act as a trustee, or in terms of IT security, as a Trusted Third Party (TTP): a (possibly non-human) entity, whom all parties trust, enforces legal obligations. These obligations ("policies") are either globally specified or attached to every single portion of data. Examples for globally specified policies are data protection laws: they are mandatory and overrule any specific policy. Examples for attached policies are user- or provider-specific requirements (e.g., "here is my driver's licence information, please, just use it for renting a car"). An example of implementing attached policies is "sticky policies" (see section 5.2.4).

However, the key factor is the ability to resolve conflicting policies. On the one hand, this ability is an important prerequisite for technically enforcing AmL, on the other hand, this is exactly the technically challenging point: to build an efficient machine (or software agent or software component) that is able to make decisions based on a defined set of rules how to act. In this context, efficient is meant in terms of autonomously acting, i.e., without the necessity of human interaction.

For a comprehensive summary of Trusted Computing with respect to the history, the objectives, the technology and the current spread, we refer back to FIDIS deliverable D3.9. At this point, we will provide a motivating example how this technology can be used as supporting technology to implement AmL.

Imagine the following two scenarios.

*Scenario 1.* Joe wants to book his next holidays and has decided to do this in the old-fashion way by going to a travel agency and negotiating the travel with a friendly travel vendor next to him. Joe wants to travel to a Greek island by air and to have a rental car at his destination. Hence, the travel vendor asks him to provide a bunch of personal data. Among these, his dietary data is needed for the airplane meals, his driving licence data for the car rental, and his passport data for the hotel registration. Clearly, Joe does not want all these data to be spread around. So, he agrees with the vendor that, e.g., the dietary information is just given to the airline. He assures that by adding a paragraph in the travel contract where this is stipulated.

*Scenario 2.* Now, let us assume that Joe wants to use a fancy, new software travel-agency-agent in order to organize his next business trip. A software agent is a piece of smart software, acting autonomously in order to fulfil a given task without user interaction. It can negotiate with other agents and make decisions. It can be regarded as actor in an Ambient Intelligence environment. Joe has now to equip his software agent with all personal data the software agent *might* need. At the same time, he defines two rules. Firstly, to each piece of personal information, a policy is attached which defines the usage permissions on his data (and possibly in which way): e.g., dietary information is just given to airlines. Secondly, data is just given to entities which technically *guarantee the enforcement* of the given policies. This guarantee (or "technical assurance") is realized by employing Trusted Computing components.

### 5.2.4 Combined approaches

To support the enforcement of privacy policies agreed on by all participants, the use of "sticky policies" has been suggested by Casassa Mont, Pearson, and Bramhall (2003). In addition to policies using formalised languages, the use of Trusted Computing has been suggested to bind the policies irreversibly to personal data through the subsequent data-processing steps and to support policy enforcement in each step. This approach also can be understood as an approach to apply digital rights management (DRM) to personal data.

In scenario II, AmI environments are partly controlled based on preferences from the data subject and supported via a device (e.g., the MyComm device as an example for a personal digital assistant). In many cases, the concepts used in these scenarios come close to user-controlled Identity Management Systems (type 3 IMS) as described in FIDIS deliverable D3.1. More realistically, it is to be expected that hybrid systems will be implemented. These combine centralised identity management (control by the operator of the AmI environment, implementing type 1 and/or type 2 IMS) with the user or data-subject-controlled identity management (type 3 IMS). In these cases, the user might get the impression to be in control, while in the background, data might still be collected and (ab)used (Bizer et al. 2006: 312ff). Therefore, besides some form of user control, transparency-enhancing tools are crucial in an AmI environment.

## *5.3 AmI-relevant TET concepts*

Whereas the previous sections gave an overview on AmI-relevant PETs, which in many cases have been realised as products, this section illustrates TETs on a concept level because implementations are missing today.

The main objective of TETs is to anticipate profiles that may be applied to a particular data subject. These profiles may be individually related to the data subject only or to groups of data subjects; they could contain personally identifiable information of the data subject, but they also may be anonymous. In any case decisions based on profiles may affect individuals, and therefore it is desired that they can know about the profiles and – if necessary – take actions if the (potential) decisions can be harmful.

In a study on linkage of digital identities (Hansen et al. 2007b), the following important roles and tasks as well as resources in the workflow of enriching data by linking them with other information are identified:

- "the address provider who assigns identifiers or addresses to a person according to an address schema defined by an address schema provider;
- the data collector who monitors and stores information;
- the linker who connects collected data items according to linking algorithms, possibly being provided by another party, the linking algorithm provider;
- the analyzer who analyzes the data by applying analysis algorithms (so-called models), possibly being provided by another party, the analysis algorithm provider (or model provider);
- the decision maker who decides on basis of the information available at that stage;
- the data subject concerned by the decision and its consequences" (Hansen et al. 2007b: 8f).

This workflow which is typical for profiling (combining linkage and analysis) shows that data as well as different algorithms (implemented in software) are needed to link and analyse the available information. If TETs should accurately mimic the profiling results which are – or can be – used by the data controller, they at best have to get access to the same data, the same linking algorithms and the same analysis algorithms which potentially take as additional input information from further data sources, possibly containing personal data of other users. These data and algorithms are not necessarily provided at one location, but different service providers may be involved, transferring their (intermediary) results to other parties involved. In many cases these algorithms are regarded as trade secrets and protected against access because the business models of specific service providers rely on them.[76] Ambitious computing power (e.g., for High-Performance Computing realised by supercomputers or computer clusters) may be required to build the profiles which is not always possible for individuals using TETs. In addition the required access to data, algorithms and computing power may require legal action (e.g. contracts to use the required resources) and course costs.

[76] In the European Data Protection Directive 1995/46/EC Art. 12 (a) explicitly mentions the data subject's right to obtain from the controller "knowledge of the logic involved in any automated processing of the data concerning him at least in the case of the automated decisions referred to in Article 15 (1)". The relation to trade secrets is touched in Recital 41: "Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;". In a German study on scoring systems (Kamp, Weichert 2006) the authors analyse that data controllers usually don't reveal the logic of their systems firstly because of trade secrets, but also to prevent data subjects from behaving differently in order to manipulate the scoring results.

Provided that TETs get access to the data and the (implemented) algorithms as they are applied by the profiling entities and that it can work with similar computing power, it will get the same results. Still, this does not automatically predict which decision the decision makers will make, basing on further factors probably not fully known by the data subject.

TETs could only access all the data and algorithms to be used if the entities doing the profiling provide this information by themselves, e.g., by allowing direct access or by involving third parties where data and software are made available, e.g., a Data Protection Authority. Even if this was legally demanded and data controllers really fulfil such a legal obligation, this would only cover the actual and planned profiling. For additional profiling done spontaneously or combining further data sources, potentially without bothering to fulfil the law (or being outside the legislation), TETs would have to "guess", i.e., collecting all kinds of (public and access-restricted) data and algorithms from various data sources and perform all kinds of data mining on the data. By this probably a vast number of different profiles related to the individual would result. The use of PETs for data minimisation would have an influence on the possible results, but still then, profiles could be calculated based on probabilities of linkage or they would be rather group profiles instead of individual profiles which also could lead to decisions directly affecting the individual concerned.

TETs would have to work all the time to generate new profiles or update already created ones because each action, whether by the individual itself or some other entities with at least some relation to the individual, could influence them. Of course the use of TETs as such is also a piece of information which can be used for profiling. Moreover, the output of TETs may affect the decisions of users: not only to prevent their privacy, but it may overwhelm them, stop them from doing anything (because it could be bad for the profiles on them) or make them careless as they feel doomed by all that information out there. These reactions can be used for further profiling again.

We conclude from the thoughts sofar that comprehensive TETs are hard to realise, and even if there were possible implementations, it would be necessary to teach individuals to use them in a way which empowers them instead of frightens or depresses them.

Still, transparency is necessary if people should be able to make informed decisions on their behaviour in the information society. So there might be some components for TETs which do not claim to really perfectly anticipate profiles, but help users at least a bit (partially already mentioned in section 5.2):

- The history logfile of past actions and data disclosures in the trusted area of an individual.
- Information for data subject on their data stored and the way of data processing by data controllers (including data transfers), possibly more detailed than in a typical privacy policy if needed.
- Information on security breaches which may lead or have led to unauthorised access.
- Publicly available collection of known linkages and linkability of data (cf. Hansen et al. 2007b).
- Computation of linkability of attributes considering explicit and implicit information (cf. Berthold, Clauß 2007).

- Publicly availably information on known profiling algorithms and implementations; if not provided by the data controllers themselves, then possibly being re-engineered by peers and provided publicly.
- Provision of computer power by peers to calculate profiles for authorised users.
- Understandable presentation of all available information.
- Media campaigns to teach individuals on what typically is being linked, how they can notice from decisions of possible profiles and categorisations and how they can react if these decisions are not desired.

In all cases when information is being provided, individuals should get the means to interpret it, e.g., by technological support and/or help of third parties or peers trusted by them.

## 5.4 Conclusion

Whereas for TETs only some components are already available yet, there exist many PET concepts and tools. Still, there is a lack of these in real usage. A few reasons for this are obvious, e.g., human computer interfaces have to be improved so that people really understand the value of using PETs in the given context and are able to handle them appropriately. Comprehensive integrated PET systems are needed if these technologies should really cover a manifold of areas in people's lives and get widely distributed.

The same is true for all those PET and TET components that show transparency information from various sources, so-called transparency tools: for being successfully employed, they would need to be handled in an integrated way to substitute today's fragmented view, provided by those available transparency tools that cover only small parts of useful information. Moreover, the given information should be accurate and easy to understand without being improperly oversimplified. In addition, large parts of these transparency tools, especially the automated privacy policies, are typically based on static and – from the perspective of data controllers – very general information. They are not designed to deal with profiles that are highly dynamic in the way of being calculated, the resulting content, and the purpose of use.

Today's existing PETs are focused on personal data and their use in compliance with privacy principles or data-protection legislation. In the context of group profiling, the link of the resulting profiles to a data subject via the underlying personal data may get lost and thus privacy principles and data-protection legislation does not apply. Nevertheless these profiles may be used to influence or direct the communication with individuals in a, from their point of view, non-transparent way. Today for these types of application of profiles no TETs are available, apart from general information about profiles and their potential use from consumer protection organisations.[77] In turn, opacity based on trade secrets is applied by organisations calculating and using such profiles.[78]

A very basic problem is that people can never be sure that they get all necessary information. In particular in the AmI world, there might be sensors that do not comply with data-protection law and that as a matter of course do not inform data subjects that they are being monitored. This problem is not new: also in former times, secret services and criminals tried to spy on

[77] For example CASPIAN, see http://www.nocards.org/.

[78] This argument is being used for example in the context of credit scoring, see FIDIS deliverable D7.2.

individuals without being noticed. This spying technology for hidden use has meanwhile become available for everybody; even daily-life devices such as mobile phones or digital cameras can be used by every individual for surveillance without informing the persons concerned. This problem can neither be solved by PETs nor TETs alone. However, it is valuable to consider findings of third parties or other peers on possible surveillance, linkage or profiling. Users should be able to choose from a plurality of information providers whom to trust with reliable information.

Obviously transparency tools (including TETs) can enhance current PETs, extending them to more comprehensive systems for dealing with privacy-relevant data and activities. However, transparency does not automatically guarantee that people are offered real and fair choices: in fact, privacy-invasive behaviour of applications could be made transparent without supporting the user in protecting his or her privacy because there is simply no choice. In this case, people should be empowered to complain via other ways, as offered by today's democratic state mechanisms, e.g., informing supervisory authorities, bringing the case to court, or using political influence.

In addition, the data collection needed for TETs can be regarded as yet another data silo which would have to be safeguarded – by this interesting data collection, even privacy and security incidents may be provoked which would not happen if data minimisation by PETs was realised properly.

Summarising, data minimisation done by PETs should be preferred over mere transparency. However, most PETs work in the world of Internet and telecommunications rather than in a comprehensive AmI setting a user lives in. Thus, there is a need for developing PETs which protect users also in the AmI world, e.g., by controlling sensors by devices in the area of the user. Transparency is a necessary mechanism for the individuals' privacy, and transparency tools should be further developed – including their human-computer interface components to help users understand what is happening and an integrative approach to offer users transparent PET solutions. From the current perspective, an accurate anticipation of profiles as intended by the TET concept is highly unrealistic because, among other things, data and algorithms are very valuable for data-processing entities and access to full information will be restricted – mainly because of trade secrets, but also because of data-protection reasons. Even if individuals can make use of some PET and TET components, organisations able to do linkage, profiling and analysis will still have more power. There may be remedies by strong involvement and support of third parties and active peers who are sufficiently trusted by the individual. Furthermore, transparency is the essence of self-determined life in society. This should be a reason for data subjects as well as Data Protection Authorities to enforce the right to access including the knowledge of logic involved in any automated processing concerning individuals. Having this and individuals trained to interpret the output of TETs – similar to what they intuitively do in the offline world –, TETs and PETs can be the tools for user's self-determination also in the ambient world.

# 6 How to achieve AmL: the architecture of the rule of law

## *6.1 The need for a paradigm shift*

Core principles of the legal data-protection framework, notably data minimisation, purpose specification, and goal binding, are entirely at odds with the vision of Ambient Intelligence. AmI cannot develop at all if the current framework is applied. It is questionable, however, whether the legal framework is powerful enough and can be enforced in practice to stop the development of AmI. More importantly, it must be questioned whether the development of new emerging technologies and AmI applications systems *should* be hindered by legal provisions based on a world view that is becoming increasingly outdated. The vision of AmI requires a revision of the legal data-protection framework as it currently exists. Nissenbaum's concept of contextual integrity (see section 3.5.2), for instance, seems more apt to protect citizens against violations of their privacy than more ‘traditional’ conceptions of privacy, which depend on a strict separation of public and private spheres.

At the same time, the core values *behind* privacy and data protection also imply that AmI should not be allowed to develop in a legal vacuum. The values that privacy and data protection aim to ensure, such as autonomy, self-development, and human dignity, must in one way or another be safeguarded in the development of the AmI world. Value-embedded design is a key notion in this process (see section 3.5.1). Where current guiding principles of the legal framework like data minimisation and purpose specification increasingly fall short, other mechanisms must be established to maintain some form of balance between users (consumers, citizens) and providers (businesses, government).

Moreover, while preventative, *ex ante* data-protection measures slowly give way to more restorative, *ex post* fair information-processing measures, also non-discrimination will become more important when AmI applications seamlessly and invisibly make customised decisions about people. A first prerequisite for non-discrimination in an AmI world is transparency, since challenging unfair autonomic decisions is only possible if it is known *that* an autonomic decision was made and *on what grounds* this was done. Such transparency will not emerge by itself, and it is unlikely that mere legislative or self-regulatory measures will entice AmI providers to create sufficient transparency for users, as long as the legislator sticks to the printed script to articulate its legal enactments. This is why Transparency-Enhancing Technologies (TETs) are a crucial element of the AmI infrastructure, as part of the *legal* infrastructure enacted by the democratic legislator.

The failure of the current data-protection framework in the face of today’s profiling and tomorrow’s Ambient Intelligence implies that a paradigm shift is needed. Both privacy- and data-protection-related values and non-discrimination require new norms when AmI is being developed, and they require rearticulation in new technologies. Because of the particularities of AmI, with its massive, real-time, self-learning, and ubiquitous profiling and decision-making, the future of these norms lies in technology itself rather than in law as we know it today. AmI norms should not – or at the very least not only – be laid down in text-based legal provisions, but they should also be embodied in the technology itself that they aim to regulate. Here, the vision of Ambient Law enters the picture.

## 6.2 Inventory of lacunae in the legal and technological framework

Ambient Intelligence is only a vision. However, the enabling technologies for AmI are being developed today. To anticipate the realisation of this vision, we need also to develop a vision of the kind of law that will safeguard autonomy and non-discrimination in smart environments that depend on real-time monitoring and proactive autonomic computing. Waiting for the realisation of AmI before developing a vision of the law that regulates AmI – Ambient Law – is not an option, because the effectiveness of AmL will depend on its inscription in the technological architecture it aims to regulate. Thinking in terms of such inscription as a matter of implementation only is also not a viable option, because the legitimacy of AmL will depend on the extent to which it conforms to both democratic processes and the rule of law. Before answering the research question of this report, we will make an inventory of the issues that need to be resolved in the legal and technological domain, if AmL is to be a success. We refer to the description of the fair information principles as part of AmL (see section 3.5.1) and compare this to solutions presented in the legal and technological chapters.

### 6.2.1 Transparency of the processing of personal data

The requirement of transparency of data processing relates to the possibility of history management of one's personal data and access to processed personal data with data controllers, to be made possible via M2M communication.

European data-protection legislation, with its focus on the protection of personal data, provides a series of rights for individual citizens and obligations for data controllers to allow citizens to access their personal data and the way they are processed. Notably, data controllers have an obligation to inform data subjects about which data are being processed, about the identity of the data controller, the purpose, and possible third parties to whom data are sold or transferred. Even today it is nearly impossible for citizens to check compliance with such obligations; in the case of AmI, the processing of data will become ever more invisible. Without intelligent agents doing the job for us, keeping up with data exchanges seems an illusion. The problem thus seems to be that even though rights and obligations exist, their realisation is a mission impossible, especially in an AmI environment. We refer to the legal analysis of FIDIS deliverable 7.3 and 7.7 for similar conclusions.

As discussed in sections 5.2 and 5.3, to exercise the right to transparency of data processing, several technological tools have been developed, notably P3P and History Management, while DRM and Trusted Computing could add alternative ways to track personal data and the way they are being processed. Such tools should be somehow embedded in a personal device, like a PDA, which enables users to interact with the environment in an automated way, while keeping substantial control over data flows, through preventing unauthorised data processing (*ex ante*) or through making data processing transparent to allow for redress procedures (*ex post*). However, two major problems arise:

- these transparency-enhancing technologies are not fully developed yet, let alone widely used;
- individual citizens cannot be sure that they actually achieve the transparency they claim to provide.

### 6.2.2 Purpose specification and use limitation

The transparency discussed in the previous section should enable one's PDA to check – M2M – which purposes are specified, and whether the principle of use limitation has been complied with in light of these purposes.

We refer to the legal and technological analysis summarised in the previous section to conclude that even if the legal obligation to specify the purpose and to restrict data processing to the purpose specified is in force (cf. section 4.3.1.2), it is nearly impossible to actually check to what extent which service provider complies with these obligations (see especially section 5.3).

We add that tools for history management that keep track of personal data after their disclosure, as discussed in section 5.2.2.2, are relatively new. It is unclear to what extent such tools can keep up with unauthorised selling of data to third and following parties. It is also unclear what happens if the data are anonymised and used for group profiling.

A device that communicates M2M with the Ambient Intelligent environment to check whether the data are in fact processed in accordance with the specified purpose has not been developed as yet (see again section 5.3).

### 6.2.3 Consent

The issue of consent has been described as enabling one's machine-proxy (the PDA that serves as a proxy when negotiating consent) to negotiate, e.g., the supply and processing of personal data according to one's personal preferences, while taking into account the mandatory aspects of data-protection legislation.

The legal chapter argues that the realisation of informed and explicit consent is highly problematic (cf. section 4.3.1.2), due to the fact that individual citizens have no idea about the consequences of the processing of their data (raising doubts as to the meaning of 'informed' in this context), while consent is often requested automatically whenever one wants to use a specific service (raising doubts as to the meaning of 'explicit' in this context). Reiterant requests for consent would in fact challenge a core feature of the vision of AmI: it’s the emphasis on invisible, ubiquitous computing.

The technological chapter addresses the issue of consent indirectly, by referring to IMS that focus on user control (cf. section 5.2). Such an IMS would consist of a PDA that follows previously installed privacy preferences, executing a user's privacy policy. However, if this device has no information as to how the data will match the group profiles that may be applied, it cannot provide any kind of informed consent. It seems that such an IMS builds on a static conception of privacy, while an AmI environment would require real-time adaptation of a person's privacy policy to anticipate potential adverse effects. Perhaps Nissenbaum's concept of 'contextual integrity' could provide for a more responsive mechanism to negotiate consent (cf. 3.5.2). IPTS' concept of digital territories could make abstract notions like consent operational, by introducing the bubble that determines which consent is given, to maintain a person's dynamic borders, using machine-readable markers, and capable of building bridges between contexts (cf. 3.5.3).

### 6.2.4 Data quality and participation

This has been described as the capability of one's machine-proxy to match data stored in data bases with one's accurate personal data, and its capability to require adjustments if data are not correct (anymore).

Without transparency, data quality and participation are empty concepts (see section 6.2.1). A PDA should be able to track and trace one's personal data and be capable of contesting data it considers either incorrect or processed in violation of mandatory data-protection legislation.

### 6.2.5 Accountability of the data controller

The requirement of accountability of the data controller implies that at all times, one's machine-proxy should be capable of *identifying* the data controller who reads, collects, stores, or otherwise processes data, including all others that have access to these data. This could be done pseudonymously, as long as there is identifiability of the data controller in case of data-protection violations.

We again refer to 6.2.1, because to hold someone accountable, one must be able to identify the culprit. Otherwise, the legal right may be in force but hardly enforceable. A PDA should refuse access to any kind of personal data if it cannot verify the identity of the data controller. Again, this could happen pseudonymously, if the user can rely on a fool-proof procedure for lifting the pseudonym in case anything goes wrong later on. In the case of AmI, this would imply that untraceable data controllers have no access to personal data whatsoever. In view of the public nature of the need to identify data controllers, it should not be left to individual choice whether a data controller can be traced. Such identification should be mandatory.

### 6.2.6 Transparency of (group) profiles used to categorise individuals

Because applying (group) profiles to individuals can have significant consequences for the individual, it should be made transparent *that* a profile is being applied and also *which* (type of) profile. Simply put, this means that one's machine-proxy should be able to monitor the environment's anticipating actions (which are based on profiles), so that she can decide on the spot whether she wants to meet the environment's action (for example, go into a café if the environment suggests she will find this enjoyable), change her behaviour (walk away from a shop window, so that the environment no longer thinks she is shopping), or complain because the profiling is based on unjust criteria (e.g., press a button of a coffee machine refusing to give her caffeine coffee, so that she can check on the machine's profiling statement whether this refusal was based on her shaking hands, which is – in her case – not a sign of overagitation but a genetic disorder, and if so, file a complaint through her PDA to the coffee machine's operator). AmI users should not have to make such decisions all of the time, of course: their PDA should learn in which cases they go along with the environment and in which cases they want to be informed of profiling in order to make a case-specific decision.

The present legal and technological framework does not provide for anything remotely like this. The focus is on hiding and keeping track of the personal data of a data subject, not on tracking the group profiles that are being inferred from other people's data. As has been extensively argued in FIDIS deliverable 7.7, profiling is *the* enabling technology of AmI, and its impact on the lives of individual citizens will be far more impressive than the impact of data collection per se. Profiling, or pattern recognition, will increase the knowledge-asymmetry between data controllers and data subjects as long a data subjects have no means to access and understand the profiles. At this moment, we lack both the legal right to access profiles and to effectively contest their application and the technological means to achieve such access, while to be able to contest their application, we need to develop some kind of understanding of the meaning of the patterns they present.

# 7 Conclusion: The potential of AmL to empower citizens in an AmI environment

The research question, formulated in section 1.2, reads as follows:

> can law as embodied in the future Ambient Intelligence architecture – Ambient Law – safeguard the core values of privacy and non-discrimination, while at the same time helping to realise the potential of Ambient Intelligence?

Having discussed the way modern law depends on the printed script, we have come to the conclusion that in a digital world, the law will need a measure of digitalisation. ICT-embedded law does not have to replace text-based, printed law – on the contrary –, but in an AmI world, 'law in the books' should be complemented with 'law in other technologies' in order to (re)gain effectiveness. The totality of text-based and technologically-embedded legal rules that regulate Ambient Intelligence is what we call Ambient Law.

The legitimacy of this digitised law will depend on its integration into the framework of democracy and the rule of law. The analysis of the previous section (6.2) has demonstrated that AmL could in fact empower citizens to stay tuned to what is going on in an AmI environment; it thereby acts as a check on AmI providers to know too much of AmI users or to make unjustified decisions about them. To a much further extent than the present legal framework, the integration of legal rights of opacity and transparency with the technological architecture would enable citizens to actually exercise these rights. Also, by developing new rights concerning the transparency of profiling practices, one of the major lacunae in the present legal framework could be resolved.

The vision of Ambient Law, as law embodied in the AmI architecture, can thus significantly help to safeguard the core values of privacy and non-discrimination, without obstructing the development of Ambient Intelligence as such. On the contrary, building in these core values into the AmI architecture will help to enhance its social and legal acceptability and will thus further the development of AmI.

Whether digitised rules also conform to principles of democracy and constitutional law, however, cannot be taken for granted. Technological embodiment of legal norms should not be confused with technological implementation of legal rules since the legitimacy of the entire enterprise will depend on its integration into the framework of democracy and the rule of law. This will be a challenging task, since the technical embodiment of rules in the AmI architecture cannot, of course, be undertaken by the legislature by itself. A plethora of public and private actors will have to work together to build the AmL architecture. It is certainly no foregone conclusion that technologically-embodied rules are democratically acceptable.[79] This will depend on the balance of legal certainty, contestability and democratic participation, while, for example, the rules should be sufficiently fine-grained and flexible to allow for the nuances that are a core element of law in practice. Private actors involved, such as software engineers, should make transparent and auditable which norms are embedded where in the AmI software, which likely can only be done with open-source software. Making technology-embedded rules meet core principles of law is a daunting task indeed.

However, this should not deter us from trying. If we give up the vision of Ambient Law from the start, then we should give up the vision of Ambient Intelligence as well, or else accept that

[79] Cf. Koops 2007 on the democratic acceptability of technology-embedded norms.

the AmI world that will be developed in the next decades has tremendous gaps in legal protection for citizens and consumers. We are not ready to accept these bleak alternatives – both the provider-centric scenario (section 2.1), with users being manipulated by ‘the system’ without knowledge or redress, and the user-centric scenario (section 2.2), with AmI not fulfilling its potential because users too often have to make data-control decisions or lack benefits because the environment is simply not intelligent enough, are not attractive visions of the future.

Since the vision of Ambient Intelligence has enormous potential for citizens and consumers, but also large risks for legal protection, we feel that the vision of Ambient Law should be developed as an important roadmap for making the vision of Ambient Intelligence come true, in such a way that core values of privacy and non-discrimination are safeguarded.

In this report we have only been able to provide a first vision of Ambient Law, outlining its basic concept. Much is needed to further develop, refine, and implement this vision. We recommend that at least the following issues are taken up for further research:

1. revising the legal framework of rights and obligations concerning privacy and non-discrimination in light of the advent of Ambient Intelligence, where core features of the current framework, like data minimisation, purpose specification, informed consent, and accountability, fall short;
2. creating an adequate legal framework for generating and applying profiles, including effective rights of access and effective rights to contest the application of profiles; this implies the development of effective transparency-enhancing tools (TETs) with regard to group profiles;
3. developing human machine interfaces that allow individual citizens to communicate with their environment, achieving (1) an adequate insight in the way they are being profiled by their environments, (2) without being flooded with information, but (3) allowing where desired to prevent or to contest application of a profile;
4. developing technological tools and redefining legal rules in such a way that the rules can be digitised and built-in in the AmI architecture, making the exercise of these rights feasible and enforceable (the concepts of 'contextual integrity' and 'digital territory' may prove fertile for such redefinition);
5. developing mechanisms for ensuring the legitimacy and conformity with core legal principles of technology-embedded rules.

# 8 Scenario III: One Upon a Time, In the Kingdom Of Ambient Law

Introduction

Li-lian is the wife of David Cragg. They have a lovely daughter, Zoe, who is 7 years old, and they have moved from the north of England to London, due to a very interesting job offer for Li-lian, who is now marketing manager at a prestigious 4-star hotel.

Scene 1: Waking up to a smart home

Li-lian wakes up to an artificial light that increases its intensity, somewhere between 5.30 and 6.30, when the smart dust within her body has registered the optimal moment to rise from sleep. Similarly, Zoe wakes up to an artificial light and some light music, adjusted to her biological profile. Li-lian suffers mildly from winter depressions, so the light's intensity remains relatively high for about 20 minutes while she prepares and enjoys a light breakfast with her daughter in the kitchen. Based on ubiquitous monitoring of her gait, eye movements, skin temperature, and specific hormonal levels, the house anticipates Li-lian’s moods and adjusts waking time, bright light duration and intensity, as well as the supplies in her fridge and larder. The house also advises her on physical exercises that improve her moods and decrease fatigue.

As Li-lian opens the fridge to replace the milk, the kitchen screen suggests that she do five more bending exercises – a welcome decrease from last month now that she managed to lose 0.424 pounds in weight last week. The house sensors also note that Li-lian is blinking rather more than usual, and since she hasn’t really had much vitamin-A-rich food lately, the KitchAid places carrots on the autonomic shopping list. Before Li-lian is off to work, she screens the shopping list and is just in time to replace the carrots – odd that the system hasn’t noticed until now that Zoe hates carrots! – with yellow peppers. When Li-lian tries to access the home network for information about her daughter’s state of mind, the network refuses access on grounds of privacy protection. Although as a parent she can override this, the system’s audit mechanism will notify Zoe, and Li-lian in this case has no good reason other than mere curiosity to explain her action to her daugther, so she decides against further intrusion.

All data that are stored and mined within the context of the home remain within the private network of intelligent agents that are running the house. These agents do not – as a default – provide external access to these data and if – after consultation with Li-lian – data are disclosed, they are tagged to trace their whereabouts and include a set of commands that restrict their use to specific purposes. The smart home network regularly checks to what use disclosed data have been put, and profiles the findings for interesting patterns.

Scene 2: Stepping into a smart outdoors

When David – who takes their daughter to school every morning – leaves the house, he steps into a whirlpool of wireless machine to machine (M2M) communication. Today, his smart car has picked up a traffic congestion on the way to school, advising him to walk or cycle to school. David decides, however, not to follow the advice and to go by car nonetheless.

Once in the car, he is tacitly aware of the permanent real-time car-to-car (C2C) communication. At a certain point, when he is distracted by persistent queries of Zoe, the car automatically slows down, even though he has actually stepped on the gas to move faster. The car has detected another vehicle at close range and anticipates a potential collision. The other day, when David drove home after a trying day at the office, the car moved into automatic pilot as the driver fatigue detector reset the default of the car. To restrict central storage of personal data of driving, most of this M2M communication around public roads does not follow a tree or star topology but runs as a mesh topology, discarding information as soon as it is outdated.

Scene 3: A smart office

When Li-lian enters her office, her chair automatically resets to accommodate the present state of her bodily fitness. Li-lian has suffered from lower back-aches ever since the birth of her daughter, and the sensor technologies and RFID systems monitor her biometric behaviour for signs of upcoming pain or fatigue. The chair has learned to which positions she responds best. In fact, her chair has detected a potential attack of lower back pain just now and forces her to continuously regain her balance (like sitting on a huge ball), because this trains the muscles and prevents a wrong posture. As she sits down and gazes at the display embedded in her desk, the desk traces all attempts from colleagues and customers to reach her and surveys all other tasks awaiting her, organising them in terms of urgency and importance, based on Li-lian's past behaviour. When the display is ready, Li-lian screens the priorities and takes some time to adjust the list, while occasionaly moving into an item to check its content.

Li-lian then takes a small break to reset her mind and starts making videocalls, skipping through reports (of which a summary has been extracted autonomically, based on pattern recognition with regard to what is deemed relevant for marketing managers in general, and personalised on the basis of her own tacit and expressed needs of information), discussing the reports with other departments and external partners, and sending them back into the content management system with tags of what she finds crucial. In the course of the day she takes a series of decisions, which feed back into the knowledge management system. Li-lian – like most marketing managers in these days – believes in open innovation, aiming for 'do your best, partner the rest'. This, of course, does not mean that she is not striving for competitive advantages; it rather indicates that she must be sharp about which information she shares with whom. The knowledge-management system continuously advises her on alternative courses of action, while her individual digital business assistant takes over negotiations whenever this is deemed more effective. Sometimes, machines come up with creative solutions their boss could not have imagined, but often, they are just used to run routine negotiations.

All personal information regarding Li-lian's health, dietary habits, and other data from which such information can be inferred is kept in a separate context. It is up to Li-lian to trade with these data or to even delete them. Information stored on the individual digital business assistant is – by default – shared with a specified set of others (meaning software agents of other employees, departments, or external partners). Both the individual private and the individual business digital assistants function as a kind of butlers or management assistants; they are professional, and relatively independent but highly dependable. At least, usually – Li-lian shudders when she recalls the latest Digital Assistant scandal, where a new operating-system release had a major flaw, enabling employers to access data in blatant violation with built-in data-protection policies. She is careful to use only digital assistants with proven trusted computing.

Scene 4: A smart school

When David arrives at school, Zoe kisses him goodbye and enters the building. The building recognises her behavioural biometrics and turns on the screen of her virtual learning environment (VLE). By the time she reaches her desk, a program for the day is already on the screen: she will have to start with math and then do some grammar. The program is based on her progress so far in relation to the end terms that have been set for this year, month, and week. After about half an hour, the program adapts to include less grammar exercises and more math, because the VLE anticipates she will make better progress this way. Her interactions are monitored, her memory and understanding are tested, and she receives real-time feedback to speed up the learning process, this time applauding her efforts in math.

Her learning schedule of this week includes periods of intense interactive learning, regarding mathematics, the bio-natural sciences, the social sciences, infonomics, cognitics, and the arts. One of the mainstream techniques she works with is designing and testing simulations of 'natural' phenomena, foreign 'natural' languages, and history. This should provide her with an adequate sense of both the resistance of reality and the plurality of its manifestations.

After some time, the VLE is shut off, tasking Zoe to get involved in real-world learning processes, and forcing her to stay tuned to her schoolmates, tutors, and the world outside the school.

When she is allowed to re-enter the VLE, she presents herself to a peergroup of pupils from different schools, categorised to have a shared background, need, or interest. She enjoys exchanging information on playing chess, one of her favorite pastimes, but she also shares information on how to tackle particular problems in her math course in order to meet the targets set for this week.

Though the VLE personalises her learning tasks to fit and elaborate her interests, it also confronts Zoe with the unexpected or undesired, in order to prevent the development of narrow and biased perspectives. Today, Zoe has to study and discuss the impact of animal testing on the researchers that perform the tests, a topic far outside her range of interest. All her personal data and profiles that are used to monitor her progress and adapt the learning environment to match her level of understanding are compiled in a protected virtual environment. The data can be mined anonymously for group profiling, including data from other schools. This has enabled a more refined understanding of a learning disability that Zoe suffers from, allowing the VLE to anticipate its negative effects by developing strategies to avoid whatever triggers the fatigue that blocks her capacity to take in more information.

When David enters to pick up his daughter, he asks her tutor to give him access to her personal profile. As he knows, he does not have unlimited access to her profile, and as she grows older he will need her permission. This is not a problem to David, who is convinced of the importance of respecting his daughter’s growing autonomy.

# Bibliography

Beckwith, R. , "Designing for Ubiquity: The Perception of Privacy." *Pervasive computing* 2003 (April-June): 40-46

Bellotti, V. and A. Sellen, "Design for Privacy in Ubiquitous Computing Environments." *Proc. of the European Conference on Computer-Supported Cooperative Work* 1993

Berman, H., J. , *Law and Revolution. The Formation of the Western Legal Tradition*. Cambridge Massachusetts and London, England, 1983, Harvard University Press.

Berthold, S., Clauß, S. , 'Linkability Estimation Between Subjects and Message Contents Using Formal Concepts', accepted at DIM'07, ACM Workshop on Digital Identity Management, November 2007, to appear in the proceedings 2007.

Bizer, J., Spiekermann, S., Günther, O. (Eds.), Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS), Berlin 2006. Download: https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf

Blavin, J. H. and I. G. Cohen , "GORE, GIBSON, AND GOLDSMITH: THE EVOLUTION OF INTERNET METAPHORS IN LAW AND COMMENTARY." *Harvard Journal of Law & Technology* (16) 2002-1: 265-285.

Brückner, L., 'Aktiver Datenschutz mit Data Journals', Datenschutz und Datensicherheit 5/2003, p. 300, Wiesbaden 2003.

Brückner, L., Voss, M., 'MozPETs – a privacy enhanced Web Browser', Proceedings of the Third Annual Conference on Privacy, Security and Trust (PST05). St. Andrews, New Brunswick, Canada; October 12-14, 2005. Download: http://www.ito.tu-darmstadt.de/projects/prima/

Bygrave, L. , Automated Profiling – Minding the machine: Article 15 of the EC data protection directive and automated profiling, *CLSR,* Vol. 17 no 1, 2001, p.17-24

Caplan, J. and J. Torpey, *Documenting Individual Identity.* Princeton and Oxford, 2001,Princeton University Press.

Čas, J., 'Privacy in Pervasive Computing Environments – A Contradiction in Terms', IEEE Technology and Society Magazine, pp. 24-33, Spring 2005. Download: http://www-personal.si.umich.edu/~rfrost/courses/SI110/paper_support/Cas,%20Privacy%20and%20Ubiquity.pdf

Casassa Mont, M., Pearson, S., Bramhall, P., 'Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services', HP Technical Reports, Bristol 2003. Download: http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf.

Chevallier, J., *L'Etat de droit.* Parijs, Montchrestien 1994.

Daskala, B. & Maghiros, I., D1gital Territ0ries - Towards the protection of public and private space in a digital and Ambient Intelligence environment, 2007, IPTS EUR 22765 EN. Available at: http://www.jrc.es/publications/pub.cfm?id=1474.

De Hert, P., "What are the risks and guarantees need to be put in place in view of interoperability of police databases?" in European Parliament. Directorate-General for Internal Policies of the Union (ed.), *Area of Justice, Freedom & Security, Collection of Standard Briefing Notes by External Experts,* Brussels 2006, Parlement Européen (Ed.).

Dommering, E. J. and L. Asscher, Eds. , *Coding Regulation. Essays on the Normative Role of Information Technology*. IT & Law Series. The Hague 2006, T.M.C. Asser Press.

Dumortier, J., "Privacy en gegevensbescherming", Vlaamse Jurist Vandaag, 1993, 6.

Eder, K., Die Entstehung staatlich organisierter Gesellschaften. Ein Beitrag zu einer Theorie sozialer Evolution. Frankfurt am Main: Suhrkamp 1976.

Eisenstein, E. , *The Printing Revolution in Early Modern Europe.* Cambridge New York 2005 (second edition) Cambridge University Press.

Flanagan, M., D. Howe, et al., Values in Design: Theory and Practice. *Information Technology and Moral Philosophy*. J. Van den Hoven and J. Weckert. Cambridge 2007, Cambridge University Press.

Friedwald, M., E. Vildjiounaite and D. Wright, SWAMI: The brave new world of ambient intelligence: a state-of-the-art review, January 2006. Download: http://swami.jrc.es/pages/documents/SWAMI_D1_Final_001.pdf.

Geisler, D. M., "Modern Interpretation Theory and Competitive Forensics: Understanding Hermeneutic Text." *The National Forensic Journal,* 1985 III (Spring): 71-79.

Goody, J. and I. Watt, "The Consequences of Literacy." *Comparative Studies in Society and History* (5) 1963-3: 304-345.

Grimm, R., Puchta, S., Müller, M., Bizer, J., Möller, J., Will, A., Müller, A., Jazdzejewiski, S., Privacy4DRM, Ilmenau and Kiel, May 2005. Download: http://www.bmbf.de/pub/privacy4drm_studie.pdf

Hansen, M., 'Marrying transparency tools with user-controlled identity management', in: Proceedings of the IFIP & FIDIS Summer School, 6-10 August, 2007 in Karlstad, Sweden, IFIP International Federation for Information Processing, Springer, to appear in 2008.

Hansen, M., Fischer-Hübner, S., Pettersson, J. S., Bergmann, M. (2007a), 'Transparency Tools for User-Controlled Identity Management', accepted for publication in the Proceedings of eChallenges, 2007.

Hansen, M., et al. (2007b), 'Verkettung digitaler Identitäten', Study commissioned by the Federal Ministry of Education and Research, Germany, 2007, in German, Executive Summary available in English, to appear.

Hansen, M., Krasemann, H., Krause, C., Rost, M., Genghini, R., Identity Management Systems: Identification and Comparison Study, Sevilla 2003. Download: http://www.datenschutzzentrum.de/projekte/idmanage/study.htm

Hildebrandt, M. , *Straf(begrip) en procesbeginsel. Een onderzoek naar de betekenis van straf en strafbegrip en naar de waarde van het procesbeginsel.* Deventer 2002, Kluwer/Sanders Instituut.

Hildebrandt, M., A Vision of Ambient Law. *Regulating Technologies.* R. Brownsword and K. Yeung, eds. Oxford 2008, Hart (forthcoming).

Hildebrandt, M. and S. Gutwirth (Eds), *Profiling the European Citizen. Cross-disciplinary Perspectives.* Dordrecht 2008, Springer (forthcoming).

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

ISTAG (Information Society Technology Advisory Group), *Ambient Intelligence: From vision to reality*, 2003, available at: http://www.cordis.lu/ist/istag-reports.htm.

Jay, R. & A. Hamilton, *Data protection – Law and Practice*, London, Sweet & Maxwell, 2003

Jiang, X., Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social. Berkeley 2002, Computer Science Division University of California.

Kamp, M., Weichert, T., Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, Study commissioned by the Federal Ministry of Food, Agriculture and Consumer Protection, Germany, 2006, in German, Summary available in English. Download: http://www.bmelv.de/cln_045/nn_752314/SharedDocs/downloads/02-Verbraucherschutz/Finanzdienstleistungen/scoring.pdf

Kranzberg, M., "Technology and History: 'Kranzberg's Laws'." *Technology and Culture* (27) 1986: 544-560.

Juels, A., Rivest, R., Szydlo, M., 'The blocker tag: selective blocking of RFID tags for consumer privacy', CCS'03, October 2003, Washington.

Kolari, P., Ding, L., Ganjugunte, S., Kagal, L., Joshi, A., Finin, T., 'Enhancing Web Privacy Protection through Declarative Policies', in Proceedings of the IEEE Workshop on Policy for Distributed Systems and Networks (POLICY 2005), June 2005. Download: http://ebiquity.umbc.edu/_file_directory_/papers/156.pdf

Koops, B.J., 'Criteria for Normative Technology. An essay on the acceptability of 'code as law' in a democratic constitutional state', TILT Law & Technology Working Paper Series 2007, No. 03/2007 (forthcoming)

Kuner, Ch., *European Data Protection Law*, Oxford University Press, 2nd edition 2007

Langheinrich, M., Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *Proc. 3rd. Int'l Conf. Ubquitous Computing*, 2001, Springer**:** 273-291

Lessig, L., "Commentaries. The law of the horse: What cyberlaw might teach." *Harvard Law Review* (113) 1999: 501-546.

Lévy, P. "Sur les chemins du virtuel." from http://hypermedia.univ-paris8.fr/pierre/virtuel/virt0.htm.

Meints, M., 'Protokollierung bei Identitätsmanagementsystemen', Datenschutz und Datensicherheit, 5/2006, pp. 304-307, Wiesbaden 2006. Download: http://www.fidis.net/fileadmin/fidis/publications/2006/DuD05_2006_304.pdf

Meints, M., Möller, J., Privacy Preserving Data Mining – a Process Centric View from a European Perspective, to be published 2007.

Müller, Günter and Kai Rannenberg: *Multilateral Security for Global Communication - Technology, Application, Business*, 1999 Addison-Wesley-Longman.

Nissenbaum, H., "Privacy as Contextual Integrity." *Washington Law Review* (79) 2004: 101-140

Oliveira, S. R. M., Zaïane, O. R., Towards Standardization in Privacy-Preserving Data Mining, Edmonton 2004. Download: http://www.cs.ualberta.ca/%7Ezaiane/postscript/dm-ssp04.pdf

PRIME Project: White Paper V2, June 2007. Download: https://www.prime-project.eu/prime_products/whitepaper/

Reinhardt, A., "Bookreview of: Gutenberg in Shanghai: Chinese Print Capitalism, 1876-1937. By Christopher A. Reed. Vancouver: University of British Columbia Press, 2004." *Technology and Culture* (46) 2005-2: 411-413.

Ricoeur, *Oneself as other*. Chicago 1992, The University of Chicago Press.

Rieback, M., Crispo, B., Tanenbaum, A., 'RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management', Proceedings of the 10th Australasian Conference on Information Security and Privacy. (ACISP 2005), Brisbane, Australia, July 2005. Download: http://www.cs.vu.nl/~melanie/rfid_guardian/papers/acisp.05.pdf

Roussos, G., D. Peterson, et al., "Mobile Identity Management: An Enacted View." *International Journal of Electronic Commerce* (8) 2003-1: 81-100

Schoemaker, P. J. H., "Scenario Planning: A Tool for Strategic Thinking." *Sloan Management Review* (36) 1995-2: 25-41.

W. Schreurs, M. Hildebrandt, E. Kindt & M. Vanfleteren, 'Chapter 13: Cogitas, ergo sum. The role of data protection law and non-discrimination law in group profiling in the private sector', in M. Hildebrandt, S. Gutwirth (eds.) *Profiling the European Citizen - Cross-disciplinary perspectives,* Dordrecht 2008 Springer (forthcoming).

Scott, J. C., Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed. New Haven and London 1998, Yale University Press.

Torpey, J., The Invention of the Passport. Surveillance, Citizenship and the State. Cambridge 2000, Cambridge University Press.

Von Mohl, R., *Die Polizei-Wissenschaft nach den Grundsätzen des Rechtsstaates*. Tübingen: Laupp 1866.

Wesel, U., *Frühformen des Rechts in vorstaatlichen Gesellschaften. Umrisse einer Frühgeschichte des Rechts bei Sammlern und Jägern und akephalen Ackerbauern und Hirten*. Frankfurt am Main, Suhrkamp 1985.

Wong, R., Data Protection Online: Alternative Approached to Sensitive Data?, *Journal of International Commercial Law and Technology,* Vol. 2, No. 1, 2007.

Wright, D., SWAMI project, Final Report, August 2006. Download http://swami.jrc.es/pages/documents/SWAMID4-final.pdf.