October 8, 2008

# Legal Safeguards for Privacy and Data Protection in Ambient Intelligence

Paul De Hert
Serge Gutwirth
Anna Moscibroda
David Wright
Gloria Gonzalez Fuster

**Paul De Hert · Serge Gutwirth · Anna Moscibroda · David Wright & Gloria Gonzalez-Fuster**

# Legal Safeguards for Privacy and Data Protection in Ambient Intelligence

**Abstract:** To get the maximum benefit from ambient intelligence (AmI), we need to anticipate and react to possible drawbacks and threats emerging from the new technologies in order to devise appropriate safeguards. The SWAMI project took a precautionary approach in its exploration of the privacy risks in AmI and sought ways to reduce them. It constructed four "dark scenarios" showing possible negative implications of AmI, notably for privacy protection. Legal analysis of the depicted futures showed the shortcomings of the current legal framework in being able to provide adequate privacy protection in the AmI environment. In this paper, the authors, building upon their involvement in SWAMI research as well as the further advancement of EU privacy analysis, identify various outstanding issues regarding the legal framework that still need to be resolved in order to deal with AmI in an equitable and efficacious way. This article points out some of the lacunae in the legal framework and postulates several privacy-specific safeguards aimed at overcoming them.

## 1 Introduction: AmI and privacy

Ambient intelligence will undoubtedly bring substantial economic and social benefits to European citizens and industry, but they will come alloyed with many risks. Heretofore, most researchers and policy-makers have drawn a rather alluring picture of these benefits for the greater good, but few have played the role of devil's advocate in trying to foresee possible problems. Nevertheless, history is littered with examples of technologies that are like the proverbial knife that cuts both ways. Thus, devil's advocates play an essential role in identifying threats and vulnerabilities. Even if it is not possible (or desirable for that matter) to bury new technologies, such as those that form the architecture of AmI, it behoves us to anticipate the threats and vulnerabilities in order to prevent them from overwhelming the many desirable features and advantages that AmI will yield. Such was the attitude of the SWAMI researchers who took a precautionary but prospective approach towards AmI. SWAMI, the acronym for Safeguards in a World of Ambient Intelligence, was a policy-oriented research project launched within the European Commission's Sixth Framework Programme. The project focused on the social, economic, legal, technological and ethical issues arising from AmI with particular regard for privacy, trust, security and identity.[1] This article summarises the many questions raised by SWAMI about the adequacy of the existing protections for privacy and personal data. In addition, this article draws upon more recent developments and considerations with regard to the EU privacy framework. It then proposes AmI-specific safeguards for privacy.

## 2 Dark scenarios

In order to identify and understand the possible implications of the technologies that are being used to construct an AmI world, SWAMI researchers collaborated with various stakeholders in developing four dark scenarios showing technology that does not work or that works in an unexpected way. The aim of focusing on such situations was to identify and highlight possible adverse impacts of and risks in AmI.[2] The four dark scenarios encompass individual-societal and private-public concerns. These concerns formed two scenario axes which helped to reduce the virtually infinite number of possible futures that could be envisaged. Following is a thumbnail sketch of each scenario:

**Dark scenario 1: A typical family in different environments** presents AmI vulnerabilities in the life of a family moving through different "spaces" – in the smart home, at work and while walking in a

[1] The SWAMI project (Safeguards in a World of Ambient Intelligence) brought together researchers from several disciplines, such as technologists, sociologists, economists and lawyers, with the aim of undertaking an interdisciplinary and holistic approach of AmI. The project finished in July 2006. Its results can be found in Wright, Gutwirth et al. [34].

[2] For more on the SWAMI dark scenarios and methodology, as well as on identified threats and vulnerabilities, see Wright, Gutwirth et al [34].

| |
|---|
| park during a lunch break. |
| **Dark scenario 2: Seniors on a journey** also presents a family, but the focus this time is on senior citizens on a bus tour. An exploited vulnerability in the traffic system causes an accident, which in turn gives rise to several travel- and health-related problems in the employed AmI systems. |
| **Dark scenario 3**: **Corporate boardroom & court case** involves a data-aggregating company which becomes victim of a theft of the personal data which it has compiled from AmI networks and which fuel its core business. Given its dominant position in the market, the company wants to cover this up but exposure by the media lands it in court two years later. The scenario also draws attention to the digital divide between developed countries that have AmI networks and developing countries that don't. |
| **Dark scenario 4: Risk society** takes place in the studios of a morning news programme, which presents three interviews involving an action group against personalised profiling, the digital divide in an environmental context and the vulnerabilities of an AmI-based crowd control system. |

## 3 Privacy threats

The ensuing analysis of each of the scenarios revealed various risks, threats and vulnerabilities posed by AmI in relation to privacy, trust, security, identity and inclusion, among which were greatly increased surveillance and monitoring, a deepening of the digital divide, identity theft, malicious attacks and so on [34]. The SWAMI partners developed a new structured methodology for analysing technology-based scenarios, the principal elements of which are a thematic synopsis of the scenario, identification of the technologies used or implicit in the scenario, identification of the applications, identification of the drivers (e.g., greed), a discussion of the issues raised in the scenario, a legal analysis and a conclusion in which safeguards are put forward.

In the following paragraphs, we draw attention to some of the issues raised by the scenarios and how AmI can put the individual's privacy in jeopardy.

### 3.1. Surveillance

First and foremost, AmI increases surveillance possibilities via omnipresent CCTV, sensor-actuators ("smart dust"), RFIDs and other technologies. These technologies make it possible to follow whatever we do and wherever we go as well as our preferences and behaviour [27]. The SWAMI scenarios show companies that monitor and track workers. They also show parents who monitor their children's digital movements [34]. RFID and similar technologies enable the Internet of things and the tracking of those things. While surveillance technologies yield apparent supervisory advantages, the downside is the oppression we feel as we are constantly monitored and our actions, if not our thoughts, are judged, which can lead some individuals to constrain their behaviour and actions to the standards accepted and preferred by the majority [17, 18, 26, 32]. This is the so-called "chilling" effect.

### 3.2. The blurring of the distinction between what is private and what is public

The lifeblood of AmI is "dataveillance", the massive collection, aggregation and algorithmic analysis of data on everyone and everything.[3] Dataveillance brings about the second big challenge for privacy protection: the blurring of boundaries between what is private and what is public. In an AmI environment, different spaces and activities overlap. The first dark scenario starts with a parent who works for a security company, mostly from his home [34]. AmI will make it easier to deal with private matters, concerning one's home life, while in the office environment or in public spaces such as parks or restaurants. The point is that technology enables us, not only to multi-task, but also to perform multiple roles (as parent, employee, friend, colleague, citizen, etc.) almost simultaneously [11]. Similarly, workers are no longer monitored just at work, but wherever they are and whatever they do. The blurring of the border between professional and home life prompts questions about how (or even if) we can distinguish between what is private and what is not, and how privacy can be protected when its boundaries are increasingly blurred?

### 3.3. Profiling

The massive collection of data by the AmI technologies that populate the intelligent environment enables extensive profiling, which in turn is necessary to deliver the benefits promised by AmI. This extensive profiling is made possible by the availability and exchange of data between various systems, devices and databases (and consequently between different spheres of one's life). AmI weaves together heterogeneous systems and devices into a seamless architecture able to accommodate the wishes of commercial agents (and governments) who want access to as much data from as many sources as possible, not only for a higher level of service personalisation, but also of security. In a hearing before the British House of Lords [16], Jonathan Faull, the European Director-General for

[3] The term dataveillance (data + surveillance) appears to have been coined by Roger Clarke in a paper he wrote entitled "Information Technology and Dataveillance", published in the *Communications of the ACM*, Vol. 31, Issue 5, May 1988.

Justice, Freedom and Security (JLS), explained that this interconnected and interoperable world is more than welcome by the law enforcement authorities and intelligence agencies, as it will contribute to the implementation of new information flows and the introduction of what they call an "Information Sharing Environment". As Mr Faull pointed out, the Information Sharing Environment (ISE) is an environment where "intelligence information should be shared between all the law enforcement agencies that are likely to find it useful". The need for such sharing of information is perceived as a principal lesson that the US authorities, but also European Member States, have learned from 9/11.

Data collection and data availability in the AmI world are not the only important issues to be examined, as we also need to consider what "knowledge" is generated from the data. Clearly, the more data, the more precise profiles. Hence, in an Internet of things, where every manufactured product is embedded with intelligence, there will be an exponential increase in data, but will it generate an exponential increase in knowledge? And, if so, who will benefit from this knowledge? Even now, such knowledge is rarely available to the individuals from whom the data are gathered. Moreover, the knowledge about citizen-consumers is often produced to achieve a certain purpose, e.g., to encourage them to buy something or to judge their eligibility for certain services (such as insurance or getting a mortgage or social services) or to assess them as a security risk. Hence, the knowledge does not match the intentions or expectations or interests of the concerned citizen-consumers. Still, the knowledge can influence the way other actors perceive the individual (or even how the individual perceives himself) [34]. Thus, the knowledge derived from AmI can create information asymmetries between those surveilled and those surveilling.

Further, this informational imbalance reflects a lack of transparency of the system towards the user, while we (the users or data subjects) are entirely transparent towards AmI (or, more specifically, the data controllers and processors).

Moreover, while the embedded environment appears to support the individual by undertaking actions on his behalf, such actions are based on his profile, e.g., the lighting in a room or temperature are adjusted to how the AmI system interprets the individual's preferences. Meanwhile, commercial offers are "personalised" to respond to what is known about the prospective consumer. However, we can imagine that the influence of AmI-induced decisions will be much more far-reaching. A transport service could be refused to a citizen categorised as potentially dangerous on the basis of information incorrectly processed. One could be refused entry into a country because the immigration authorities distrust him or her as a result of a lack of available information, as shown in the third scenario [34]. All in all, technological devices make decisions and undertake actions that affect our lives while we might not even be aware such decisions are being taken, and may learn about them only when the negative consequences become apparent. The FIDIS consortium[4] envisaged a scenario in which an individual is manipulated by AmI in many aspects of life, without his realising it [23].[5]

### 3.4. Converging technologies and the exponential increase of available data: RFID as an example

The impact of AmI upon privacy is rendered especially evident from an analysis of particular technologies. Although many of them (such as surveillance cameras, RFID and implants) have been around for a long time, the major change results from their massive deployment and interconnection. RFID is a good example: it enables communication between things (objects and readers) as well as real-time monitoring of the environment and automated decision-making.

Although RFID technology can provide significant benefits for tracking shipments, inventory management, sales and market analysis, its identification, profiling and monitoring capabilities have raised concerns, particularly with regard to its tagging of personal items. As it enables the tracking of objects, it can also – indirectly – lead to the tracking of people once the link between the person and the item is established. As each item will have its unique "identity", profiling is possible even if the real identity of the person remains unknown. Indeed, an RFID chip's serial number can serve as an identifier although no connection with the real identity of the person is made (e.g., when a tag contains a unique identifier that allows a person to be identified as an owner of the item[6]). RFIDs can be linked with individuals in many ways. For example, the Oyster card used for payment of trips on the London Underground records each trip a person makes, the stations of entry and of exit, and the time and date. If someone pays for the Oyster card with a credit card, the relation between the RFID, the information it records and the individual is cemented firmly in place. The many uses of RFID tags thus raise several questions. How should one distinguish which and what kind of information relates to a thing and

[4] FIDIS (Future of Identity in the Information Society) is a multidisciplinary Network of Excellence supported by the European Commission's Sixth Framework Programme (http://www.fidis.net/home/).

[5] This refers not only to privacy, but also to the question of the transparency of the systems and the access to the generated knowledge that would allow the individuals to be aware of mistakes, understand the decisions taken and react if they feel the decisions are wrong, discriminating or too intrusive. Crucial here are the means individuals have at their disposal to remain in control of their data and their empowerment in the new environment.

[6] The stable connection between the item and the individual is then necessary. It is possible to establish such a link in the case of personal products carried by their owners. The Article 29 Data Protection Working Party illustrated such a situation and the attendant concerns raised thereby in its document on RFID [2]. However, such a stable link between the item and the owner has been contested. See Hildebrandt and Meints [24].

which to a person? What should be regarded as personal information? Is the categorisation of information generated from RFIDs valid in other contexts where other technologies are used? In an environment where different pieces of information can easily be exchanged, linked and analysed in order to derive to certain "knowledge", how should the "raw" information, the data be categorised? Will the EU data protection rules apply? How should more sensitive information be distinguished from less sensitive information? How should personal information be distinguished or separated from other data when a single piece of data can actually disclose more information than previously expected?[7]

## 4 The legal framework and AmI: lacunae and weaknesses in privacy and data protection law

In Europe, the protection of private life and home is guaranteed by international treaties and declarations.[8] The most relevant is the European Convention on Human Rights (ECHR) [36], Article 8 of which provides for a right to privacy. Within the European Union framework, privacy and data protection have been recognised as fundamental rights in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union [38]. Respect for privacy and data protection is also regulated in several specific directives, namely the Data Protection Directive [39], E-Privacy Directive [40], Data Retention Directive [41], and the national laws of the Member States.

This regulatory framework was tested against the particularities of an AmI environment in the analysis of the SWAMI scenarios. Among the conclusions of the analysis were that AmI can effectively put the individual's privacy into jeopardy and that the existing framework appeared to offer insufficient protection of privacy and personal data.

### 4.1. AmI v. privacy protection

Above, we said that AmI blurs the boundaries between the public and the private. Is it still possible to sustain a legal distinction between these two spheres? How should legal rules be applied to protect the private home and life in an environment where there are no clear boundaries between what is private and what is public? How should individual privacy be balanced against other legitimate interests and social values in an AmI environment when the actors assume multiple roles, execute various tasks and cross various spaces at the same time [11]? The deployment of AmI technologies casts doubt on the extent to which privacy is legally protected in public spaces, including, for example, the workplace where employers can easily interfere with or intrude upon the privacy of employees.

In case law, the European Court of Human Rights has introduced the notion of "reasonable expectation of privacy". This notion has had an important impact on the evolution in legal understanding of privacy. In the case of Copland v. the United Kingdom [46], the Court ruled that monitoring or controlling personal calls, e-mails and Internet use interfered with a European citizen's right to privacy. By refuting the home v. work distinction on the basis of what constitutes a reasonable expectation of privacy, the Court has established a privacy framework that should be able to cope with some of the problems identified by the SWAMI research. Individuals can expect their privacy to be protected in public spaces (such as at work), but such protection is not without limits.[9] It remains unclear how far such protection goes, what it covers and particularly how such "reasonable expectation" can be construed. As it makes privacy protection dependent on contextual factors, it could imply that the factual evolution and introduction of new technologies will determine what privacy level can be reasonably expected, inducing a weakening of privacy protection. Is it reasonable to expect any privacy when everything we do can be constantly monitored? The development of monitoring technologies and the increasing concern for public safety and security certainly lead to the erosion of privacy: the reasonable expectation of privacy turns into an expectation of being monitored.

Moreover, there is a lack of clarity concerning the consequences of violation of privacy: while the European Court of Human Rights is willing to extend privacy protection to the workplace and public places, it rejects the exclusionary rule, i.e. the right to have evidence obtained through privacy violations excluded by the courts.[10]

### 4.2. AmI v. data protection law

The fact that AmI needs as many data as possible to achieve its full potential clearly clashes with some of the main principles of data protection law, namely, the data minimisation principle[11] (collecting as little data as necessary for a given purpose) and the purpose specification principle[12] (the collected information can only be used for the purpose defined at the moment of

[7] Information about an object and its environment (e.g., humidity) can actually contain information on a person. We refer here, inter alia, to an example given by a speaker at the UbiComp Workshop 2007 [19], and subsequent discussion of participants.

[8] In particular, the Universal Declaration of Human Rights 1948 [35], Article 12, and the International Covenant on Civil and Political Rights 1966 [37], Article 17.

[9] In Niemitz v. Germany [42], the European Court of Human Rights stated that there is no reason why the notion of "private life" should be taken to exclude activities of a professional or business nature. In Halford v. United Kingdom [43], Miss Halford, a senior officer whose telephone calls were intercepted without warning, was granted privacy protection in her office space, although not absolute protection.

[10] In cases such as Khan [44] and P.H. & J.H. v. the United Kingdom [45], the European Court of Human Rights decided that a violation of ECHR Article 8 had taken place, but it nevertheless accepted the use of the evidence in a criminal process.

[11] Article 6 of the Data Protection Directive.

[12] Article 6 of the Data Protection Directive.

data collection). In AmI, the purpose for collecting the information is often not known beforehand, not to the data subject, not to the service provider.

Moreover, surveillance technologies and extensive profiling possibilities further increase the availability and exchange of data between various systems and devices (and, consequently, between different spheres of one's life). Commercial interests and security claims provide strong incentives for more extensive profiling, while interoperability entails an unlimited availability of personal data. Such developments put data protection law under heavy pressure, especially its marrow, the purpose specification principle, which only allows processing of personal data for an explicit purpose, defined at the moment of collection of the data.

AmI also causes major problems for the consent principle in data protection law: currently, the unambiguous consent of the data subject is the main factor making a processing of personal data legitimate.[13] AmI purports to improve the quality and richness of life for the user, but it uses technologies that collect data unobtrusively, automatically, pervasively and invisibly. Requiring the user's active involvement each time data are collected goes against the logic of AmI. Moreover, in many situations, it remains unclear what an unambiguous and informed consent means, and how it should be expressed, especially when the scope of the ongoing collection of data cannot be precisely foreseen by the parties.

Furthermore, AmI technologies will confuse the difference between personal and other data. The data on a device may reveal information about the owner; data on features of the ambient environment can reveal information about its inhabitants. Again, the knowledge that can be derived from data cannot be fully determined at the moment of collection.[14] This leads to a fundamental question for data protection: how can or should personal data be distinguished from other data? The current data protection framework applies only when personal data are being processed. The definition of personal data is a very problematic notion in AmI.[15] AmI forces us to reflect on this definition – for it might turn out to be unworkable in the future. What kind of legal framework can protect private information in a way which shows resilience towards technological developments the ramifications of which are not fully known? Can a distinction between personal and other data be sustained in an AmI world? The current EU legal framework distinguishes between different categories of data, and applies a stricter protection regime towards the sensitive data. However, can a distinction between sensitive and non-sensitive information still work in AmI? Already, today, simple information on consumption habits can reveal sensitive personal data, e.g., relating to one's health or medical condition. Moreover, the perception of what constitutes sensitive data is context dependent.

The problem with the notion of personal data has already been acknowledged in the context of RFID technology. The rules of data protection apply if the data on the tag can lead to identification of a person. However, a problem might arise if such identification is not possible in a straightforward way, but is possible if the data on the tag are compared to other available data[16], or if the RFID chip's serial number serves as an identifier even though no direct link with the real identity of the person is made (e.g., when a tag contains a unique identifier that helps to identify the owner of the item). Currently, no law addresses such situations, even though the link can be used to conduct profiling and monitoring activities. Moreover, no rules address RFID systems specifically, except for some recent codes of conduct (see below).

AmI forces us to reconsider our understanding of current privacy and data protection law. It forces us to seek more flexible ways of articulating AmI requirements and concerns related to privacy and data protection, and the implied values of autonomy, self-determination and liberty. The need for new and AmI-specific legal tools must be pondered.

[13] Article 7 of Data Protection Directive [39].

[14] Such correlated information can offer a comprehensive picture of the individual. See Hildebrandt, M [21].

[15] The Data Protection Directive [39] applies to the processing of "personal data", defined as any information relating to an identified or identifiable natural person ("data subject"). Article 2 of the Directive defines an identifiable person as 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 psychic, psychological, mental, economic, cultural or social identity.

[16] The Data Protection Directive's definition of personal data can be assumed to cover the data stored by a tag for the purpose of identification (e.g., tags in passports or identity cards), or when a reference database can be used for making a connection between information on a tag and an individual. However, taking into account the increasing availability of data, as well as computing and data mining capabilities, it is possible to establish such links between information on a tag and the identity of an individual even in the absence of direct reference data. On this point, see, for example, Hildebrandt and Meints [24]. In the context of RFID and similar technologies, the usefulness of the concept of personal data can be contested. The Article 29 Data Protection Working Party states in its Working document on data protection issues related to RFID technology [2] that, if the processing of data collected via RFID systems is to be covered by the Data Protection Directive, we must determine whether such data relates to an individual, and whether such data concerns an individual who is identified or identifiable. In assessing whether information concerns an identifiable person, one must apply Recital 26 of the Data Protection Directive, which says that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". And further: "Finally, the use of RFID technology to track individual movements which, given the massive data aggregation and computer memory and processing capacity, are if not identified, identifiable, also triggers the application of the data protection Directive." This case-by-case approach was upheld in a recent document from the Article 29 Data Protection Working Party on the definition of personal data [1].

## 5 A Legal framework for AmI: specific safeguards for privacy and data protection

As ambient intelligence challenges existing legal protection of privacy, conceiving legal safeguards has become a priority.[17]

### 5.1. A good combination of legal tools

The existing legal framework (see supra, point 4) contains some important safeguards for privacy and data protection. By default, privacy law protects the *opacity* of the individual, while data protection, also by default, calls for *transparency* of the processor of personal data. We draw attention to the important distinction between opacity and transparency tools in privacy and data protection.

The traditional regulatory approach mainly focused on the use of opacity tools which proscribe interference by powerful actors into the individual's autonomy. Privacy law contains such opacity tools. However, we envisage a new paradigm where the default position will be the use of transparency tools which accept interfering practices under certain stringent conditions which guarantee the control, transparency and accountability of the interfering activity and actors. Data protection law [13, 14, 18] offers such transparency tools. If the goal of regulation is to control or channel the exercise of power rather than to restrict it, then transparency tools seem more appropriate than opacity tools. In such situations, the collection and processing of data would thus be allowed, but made controllable and controlled. Transparency tools could offer a solution to some of the legal problems raised by AmI. Other problems, however, may require a good combination of both transparency and opacity tools, as we discuss in the following paragraphs.

### 5.2. Transparency tools

A key issue in ambient intelligence is how to ensure that data collection and data processing are transparent to the data subject and how to ensure a proper balance between the information provided to data subjects and the information taken from them. In other words, how can we remedy information asymmetries where we are transparent to data processors while they remain opaque to us?

The current legal framework requires that data subjects be informed about the ways data collection and processing are organised and carried out. Nevertheless, it is questionable whether such information requirements truly give the data subject a comprehensive view of how his or her data are processed and the implications arising therefrom, especially as the amount of information might be such that, in practice, it prevents him from obtaining any really useful knowledge. Thus, we should seek simplified ways of information exchange and useful tools for information management.

Examples of simplified ways of informing the data subject about the presence of invisible, embedded AmI technologies include pictograms and simplified notices. The Article 29 Working Party has developed guidelines and proposed multi-layered information notices [3, 30]. Industry and law enforcement agencies should consider the utility of these guidelines and simplified notices.

Advancements in information technology itself could provide important factual means of transparency. Complementary to privacy-enhancing technologies (PETs), which aim at controlling the dissemination of data, transparency-enhancing technologies (TETs) [23] could contribute to information exchange and management. An example of a TET is the so-called "sticky policies" that stick to or follow data as they are disseminated. Sticky policies would provide clear information and indicate to data processors and controllers which privacy policy applies to the data concerned [10, 30]. Sticky policies would facilitate the auditing and self-auditing of the lawfulness of data processing by data controllers.[18] Another example is intelligent agents (software) that would help manage the large amounts of data processed in an AmI world.

We also need to consider how a transparency approach could help address the problem of profiling and automated decision-making. Should the data subject have access not only to the data on which profiling is based, but also to the knowledge derived from the data? Providing access to their profiles could help data subjects understand why their AmI environment undertakes certain actions. Intelligent agents could alert them to incorrect information which could influence their profiles or any improper operation taking place, and make them aware of the decisions made on the basis of the profiles. Access to their profiles could also help data subjects in proving liability in case of damage, and in shielding them against manipulation, as they would be able to contest the logic underlying the profiles and the decisions taken. Access to profiles may require some

[17] For a broader overview of legal safeguards in the field of privacy and data protection and in other legal fields, see Wright, Gutwirth et al [34]. The SWAMI consortium also proposed some general safeguards addressing issues concerning the regulation of AmI. The SWAMI and FIDIS research [24, 34] made it clear that a comprehensive approach is needed to protect privacy and that such a comprehensive approach should also address related issues such as liability and antidiscrimination rules.

[18] For example, such an approach was adopted by the PAW project (Privacy in an Ambient World), which developed the language enabling the distribution of data in a decentralised architecture, with the use of sticky policies attached to data providing information on what kind of use has been licensed to the particular actor (licensee). Enforcement relies on auditing. See http://www.cs.ru.nl/paw/results.html. The FIDIS consortium considered automated management of data and control of privacy policies. See Schreurs et al [33]. The PRIME project also discussed the matter. See Hansen et al (eds.) [20]. See also the UbiComp 2007 presentation by Le Métayer [7]. Management and auditing possibilities offered by technology should be coupled with effective liability for breach of privacy rules.

reconciliation of the right to have access to profiling knowledge (which might be construed as a trade secret in some circumstances) with the intellectual property rights of the data controller.

### 5.3. A new opacity tool – the digital territory

Even if transparency is the default position, a balanced approach might also require certain opacity measures (prohibitions of violations of privacy) in order to safeguard the individuals' autonomy and to protect them against inappropriate surveillance and discrimination.

Opacity measures could include a prohibition against surveillance in certain spaces or situations (e.g., in bathrooms) or restrictions on the use of implants or on certain exchanges of information. As for increased interoperability and profiling, they should not be considered as purely technical issues. Their multiple political, legal and economical implications must be taken into account. There is a difference between the power to connect and process personal data, on the one hand, and the desirability and acceptability of those actions, on the other hand. Basically, personal data that were not meant to be merged and made available (at the moment of collection) should not be subjected to these operations [12, 18].

Nevertheless, the fact that AmI will bring new threats brings the concomitant requirement to devise some AmI-specific safeguards. An example of an AmI-specific opacity tool is the concept of "digital territory", a concept that introduces the notion of protective borders in future digitised everyday life.[19]

The concept of digital territories aims to provide individuals with the right to privacy in a highly networked and digitised world. This private digital space can be considered as an extension of the home that would "follow" the individual in cyberspace, like an unlinkable and invisible bubble. The user would have the ability to determine the borders of his digital territory. Similarly, the individual would determine the opacity or transparency of his digital territory bubble.[20] The bubble would be like a sort of membrane managing the information flow to and from the user.

People already process their personal data on servers (files, pictures, correspondence), communicate through the Internet, disseminate personal information and content while online. The engagement of individuals in such activities will continue to increase, with the consequence that more of our private activities will move online, thereby linking more strongly our "real" and virtual lives.

It is questionable whether the law guarantees a sufficient and workable protection of our online private spaces [5, 6, 11]. For instance, the Data Retention Directive requires telecommunication service providers to keep communication data at the disposal of law enforcement agencies [41], while it is unclear whether any effective guarantees for the individual are in place when the data are being accessed.

In almost any interaction, we disclose something about ourselves, but we should be able to control what is disclosed. The digital territories concept lets individuals decide for themselves if or how much personal information they disclose, to whom and for what purpose. They could "tag" private data for follow-up purposes [11].

If such virtual private digital territories are to become effective, they must be legally defined and protected. The law should protect against unwanted and unnoticed (surreptitious) interventions by private parties or public actors, just like it ensures the inviolability of the home. A set of legal rules could be envisaged to that end, including procedural safeguards similar to those applicable to the home, e.g., requiring a duly authorised search warrant [13]. Technical solutions aimed at defending private digital territories against intrusion should be encouraged and, if possible, legally enforced [9]. Privacy-enhancing technologies, transparency-enhancing technologies and development of identity (information) management systems are all important elements in a digital territories policy.[21] The policy could also extend protection to the digital movements of the person, just as the privacy of the home is extended to one's car [13]. Protection could also be envisaged for home networks linked to external networks.

### 5.4. Specific recommendations regarding RFIDs

In addition to considering the legal questions raised by AmI as a whole, we must consider recommendations with regard to specific technologies, such as RFIDs.[22]

The Article 29 Working Party has already presented some guidelines on the application of the principles in EU data protection legislation to RFID [1]. It stresses that the data protection principles must always be complied with when RFID technology leads to the processing of personal data (although, as noted previously, it might be difficult to interpret the definition of personal data in the context of RFID technology). Hence, the individual should always be informed of the presence of tags and readers, the purposes for which data are collected and processed, who is the responsible controller, whether the data (and what kind of data) are stored, the means to access and rectify data, and whether the data will be made available to third parties.

As providing such information might be rather complicated and burdensome for both users and data processors, it might suffice to fall back upon adequate and simplified notices informing individuals about the

[19] See: Beslay, L, and Hakala, H [5]. An in-depth analysis of the concept and the various categories of digital territories can be found in a recent IPTS report by Daskala et al [11].

[20] *Idem*.

[21] An overview of the existing identity management systems has been given by Bauer et al [4]; Hildebrandt and Backhouse (eds.) [22] and Müller et al [31]. Development of identity (information) management systems has been discussed in Hansen et al [20], Leenes et al [28] and within the FIDIS project (See Schreurs et al [32]).

[22] For more on RFID safeguards, see Wright, Gutwirth et al [34].

presence and the activity of tags and readers, and the policy of the data processors (e.g., pictograms or similar). Such information should always be provided to consumers when RFID technology is used, even if a tag does not contain personal data in itself.[23] It should be possible for the data subject to disable or remove a tag, in line with the consent principle of data protection law, and the individual should, in principle, be allowed to withdraw his consent.

Privacy by design is of crucial importance in designing any technological application, and it is no less true of RFID tags. Efforts to develop technical specifications and privacy standards should continue.[24] Privacy impact assessments (PIAs) should be performed to identify all potential risks of each particular RFID application. PIAs could be a legally binding obligation. The SWAMI consortium also recommended further research into RFID technology, its implications for privacy and a reflection on possible legal safeguards.[25] Further development of codes of conducts and good practices were also recommended.[26]

## 6 Conclusions

In order to fully enjoy the benefits of AmI, we must consider its "dark" side. The SWAMI consortium identified various threats and vulnerabilities affecting privacy and data protection in AmI, including a number of weaknesses in the existing legal framework. A new approach to privacy and data protection is needed, based on control and responsibility rather than on restriction and prohibition. This article presented a few examples of legal safeguards against the loss of privacy. We discussed some possibilities for improving the transparency of the processing of AmI-generated data and for improving the control of such by the user. We also explored the concept of digital territories as one that could ensure the individual's control of his privacy despite the blurring of the borders between the private and public spheres and despite the continuing erosion in privacy. Specific safeguards for RFID were presented as an example of a precautionary approach toward a particular AmI technological application. The safeguards mentioned in this article should not be regarded as a closed list. On the contrary. AmI harbours all sorts of legal complexities. Hence, it merits further research on how to strengthen existing regulatory safeguards and devise new ones to meet the challenges before us in the brave new world of ambient intelligence.

[23] As already mentioned, such information on a tag can be a unique identifier enabling profiling activities. See Kardasiadou et al [25].

[24] Some standards have already been adopted in the RFID domain. The International Organization for Standardization has developed sector-specific standards, as well as more generic standards. Some standards have also been developed by EPCglobal (http://www.epcglobalinc.org/home), an industry-driven organisation, creating standards to connect servers containing information relating to items identified by EPC (Electronic Product Code) numbers.

[25] Researchers and legislators should also seek further solutions addressing the issue of profiling enabled by such technologies. See supra: "Dangers of AmI Enabling Technology – RFIDs"; see also Hildebrandt and Meints [24].

[26] An example of such (emerging) initiatives are the EPCglobal Ltd. guidelines regarding privacy in RFID technology [15] and the CDT (Centre for Democracy and Technology) Working Group on RFID Privacy Best Practices [9].

## References


1. Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data. 2007, (01248/07/EN WP 136) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
2. Article 29 Data Protection Working Party: Working document on data protection issues related to RFID technology. 2005, (10107/05/EN WP 105). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf, last consulted 02.07.2007.
3. Article 29 Data Protection Working Party :Opinion on More Harmonised Information Provisions, 2004, (11987/04/EN - WP 100). http://ec.europa.eu/justice_home/fsj/privacy/.
4. Bauer M., Meints, M., Hansen, M. (eds.): Structured Overview on Prototypes and Concepts of Identity Management Systems, FIDIS (Future of Identity in the Information Society) Deliverable D3.1, 2005. http://www.fidis.net

5 Beslay, L., Hakala, H.: Digital Territory: Bubbles, 2003. (draft version available at http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf), last consulted 02.07.2007

6. Beslay, L. Punie, Y.: The Virtual Residence: Identity, Privacy and Security. In: Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), 2003. http://ftp.jrc.es/eur20823en.pdf, last consulted 02.07.2007.
7. Bryce, C., Dekker, M.A.c., Etalle, S., Le Metayer, D., Le Mouel, M. F., Minier, M., Moret-Bailly. J., Ubeda, S.: Ubiquitous Privacy Protection- Position Paper. In: Bajart, A., Muller, H., Strang, T. (eds.): UbiComp 2007 Workshops Proceedings, Innsbruck, Austria, September 2007, pp. 397-402.
8. Borking, J.: RFID Security, Data Protection & Privacy, Health and Safety Issues. Presentation made during European Commission Consultation on RFID, Brussels, 2006.
9. CDT (Centre for democracy and technology) Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology, Interim Draft, 2006. http://www.cdt.org/privacy/20060501rfid-best-practices.php, last consulted 02.07.2007.
10. Casassa Mont, M., Pearson, S., Bramhall, P., Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforcable Tracing Services, HP Labs Technical Reports, HPL-2003-49, Bristol 2003. Download: http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf
11. Daskala, B., Maghiros, I.: Digital Territories: Towards the protection of public and private spaces in a digital and Ambient Intelligence environment. 2007, EUR 22765 EN http://www.jrc.es/publications/pub.cfm?id=1474
12. De Hert, P.: What are the risks and what guarantees need to be put in place in view of interoperability of police

databases? Standard Briefing Note 'JHA & Data Protection', No. 1, produced on behalf of the European Parliament, 2006.
13. De Hert, P., Gutwirth, S.: Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence. In: Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), 2003. http://ftp.jrc.es/eur20823en.pdf, last consulted 02.07.2007.
14. De Hert, P., Gutwirth, S.: Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In: Claes, E., Duff, A., Gutwirth, S. (eds.): *Privacy and the criminal law*. 2005, Antwerp/Oxford, Intersentia.
15. EPCglobal Ltd. guidelines regarding privacy in RFID technology,http://www.epcglobal.org/public_policy/public_policy_guidelines.html, last consulted 02.07.2007.
16. Faull, J., heard by the House of Lords, Minutes of Evidence taken before the Select Committee of the European Union (Sub-Committee F), The EU-US PRN Agreement, 22 March 2007, p. 5.
http://www.publications.parliament.uk/pa/ld/lduncorr/euf220307_2.pdf, last consulted 02.07.2007.
17. Gutwirth, S.: Privacy and the information age, Lanham/Boulder/New York/Oxford, Rowman & Littlefield Publ., 2002, 158 p.
18. Gutwirth, S., De Hert, P.: Regulating profiling in a democratic constitutional state M. Hildebrandt & S. Gutwirth (eds.): *Profiling the European citizen. Cross disciplinary perspectives*, Springer Press, Dordrecht, 2008**,** 271-291
19. Han, J., Shah, A., Luk, M., Perrig, A.: Don't Sweat Your Privacy, Using Humidity to Detect Human Presence, In: Bajart, A., Muller, H., Strang, S. (eds.): UbiComp 2007 Workshops Proceedings, Innsbruck, Austria, September 2007, pp. 422-427.
20. Hansen M., Krasemann, H. (eds.): Privacy and Identity Management for Europe - PRIME White Paper - Deliverable 15.1, 2005.
21. Hildebrandt, M., "Profiles and correlatable humans", in N. Stehr (ed.), Who Owns Knowledge? New Brunswick NJ, Transaction Books, 2006.
22. Hildebrandt M. Backhouse, J., (eds.): Descriptive analysis and inventory of profiling practices, FIDIS (Future of Identity in the Information Society) Deliverable D7.2, 2005. http://www.fidis.net
23. Hildebrandt, M., Koops, B.J., (eds.): A Vision of Ambient Law, FIDIS (Future of Identity in the Information Society) D7.9, version as of 15.11.2007 (http://www.fidis.net).
24. Hildebrandt, M., Meints, M. (eds.): RFID, Profiling, and AmI, FIDIS (Future of Identity in the Information Society) Deliverable D7.7, 2006. http://www.fidis.net.
25. Kardasiadou, Z., Talidou, Z..: Report on Legal Issues of RFID Technology, LEGAL IST (Legal Issues for the Advancement of Information Society Technologies) Deliverable 15, (2006).
26. Lahlou, S.: Living in a goldfish bowl: lessons learned about privacy issues in a privacy-challenged environment, Workshop on UbiComp Privacy, Privacy in Context, 2005.
27. Lahlou, S, Langheinrich, M., Rocker, C.: Privacy and Trust Issues with Invisible Computers, Communications of the ACM, March 2005/Vol. 40., No. 3, pp. 59-60.
28. Leenes, R., Schallabock, J., Hansen, M.: Prime white paper v2., 2007. https://www.prime-project.eu/prime_products/whitepaper/, last consulted 02.07.2007.
29. Maghiros I., Punie Y., Delaitre S., De Hert P., Gutwirth S., Schreurs W., Moscibroda A., Friedewald M., Lindner R., Wright D., Vildjiounaite E. & Allahuhta P., Safeguards in a world of ambient intelligence' in *The 2nd IET International Conference on Intelligent Environments*, Athens, National Technical University, conference book, 2006, vol. 2, 245-249
30. Meints, M.: AmI – The European Perspective on Data Protection Legislation and Privacy Policies, presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006.
31. Müller G. and Wohlgemuth, S., (eds.): Study on Mobile Identity Management, FIDIS (Future of Identity in the Information Society) Deliverable D3.3., 2005. http://www.fidis.net
32. Rouvroy, A.: Privacy, Data Protection, and the Unprecedented Challenges of Ambient Inteligence, September 11, 2007, available at SSRN: http://ssrn.com/abstract=1013984
33. Schreurs, W., Hildebrandt, M., Gasson M., Warwick, K., (eds.): Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence, FIDIS (Future of Identity in the Information Society) Deliverable D7.3, 2005. http://www.fidis.net
34. Wright D., Gutwirth S., Friedewald M., Punie, Y. Vildjiounaite, E., (eds.) *Safeguards in a World of Ambient Intelligence*, Springer Press, Dordrecht, 2008**,** 291 p.

**Legal Acts**

35. Universal Declaration of Human Rights, United Nations, 1948.
36. European Convention on Human Rights of 4 November 1950
37. International Covenant on Civil and Political Rights, United Nations, 1966,
38. Charter of Fundamental Rights of the European Union, *OJ* C 341, 18.12.2002, pp. 1-22.
39. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, OJ L 281, 23/11/95, pp 31-50.
40. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31/07/2002, pp. 37-47.
41. 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, *OJ* L 105, 13/4/ 2006, pp. 54-63.

**Case Law**

42. ECHR, Niemitz v. Germany (23.11.1992).
43. ECHR, Halford v. the United Kingdom (27.03. 1997).
44. ECHR, Khan v. the United Kingdom (12.03.2000).
45. ECHR, P.H. & J.H. v. the United Kingdom (25.12.2001).
46. ECHR, Copland v. the United Kingdom (3.04. 2007).