The awareness of Privacy issues in Ambient Intelligence

Mar López[a], Juanita Pedraza[b], Javier Carbó[a], José M. Molina[a]
[a] Computer Science Department, Carlos III University of Madrid
[b] Public State Law Department, Carlos III University of Madrid
{mariamar.lopez, javier.carbo, jose.molina}@uc3m.es
jpedraza@der-pu.uc3m.es

KEYWORD

Ambient Intelligence
Intelligent Environment
Privacy Issues
Privacy Policies
User's domain
Design by Privacy
Privacy Management System
Privacy Enforcement Controller

ABSTRACT

Ambient Intelligence (AmI) involves extensive and invisible integration of computer technologies in people´s daily lives: Smart Sensors, Smart Phones, Tablets, Wireless Sensor Network (Wi-Fi, Bluetooth, NFC, RFID, etc.), Internet (Facebook, WhatsApp, Twitter, You Tube, Blogs, Cloud Computing, etc.). The Intelligent Environments (IE) collect and process a massive amount of person-related and sensitive information.

The aim of this work is to show the awareness of privacy issues in AmI and to identify the relevant design issues that should be addressed in order to provide privacy in the design of Ambient Intelligence's applications focused in the user´s domain and involved technologies. We propose a conceptual framework in order to enforce privacy that takes care of interaction between technologies and devices, users and application´s domain with different modules that contain different steps relating to the privacy policies.

1 Introduction

Over the last three decades, personal data have come to play an increasingly important role in our economics, societies and everyday lives. The potential uses of personal data have increased tremendously us a result of the wide range of analytics that can provide comprehensive insights into individual´s movements, interests, and activities. At the same time, the abundance and persistence of personal data have elevated the risks to individual´s privacy. Personal data is increasingly used in ways not anticipated at the time of collection. Almost every human activity leaves behind some form of digital data trail, rendering it increasingly easy to monitor individuals´ behavior. These increased risks signal the needs for more effective safeguards in order to protect privacy.

At the beginning of this century the fast technologic changes and the globalization are giving rise new challenges and new opportunities for governments and citizens over the world, and the privacy is being increasingly the focus of attention excelling as a fundamental social value to be considered. The continuous evolution of social media increases the awareness of privacy issues. As awareness turns into concerns, users will realize that they will not be able to manage all their privacy handling themselves. They will need to find a trusted provider that can help them safeguard their privacy. Today, privacy is already becoming a value to quality for users. Users must understand what they are doing and how their personal information is being used in a specific application.

The Ambient Intelligence [ISTAG, 2001], [ISTAG, 2002] consists in the creation of living environments (called Intelligent Environments, IE) [ISTAG, 2003] where users interact in a natural and intuitive way with computational services which ease the completion of the user´s everyday tasks, being this for leisure, help or work assistance [WEISER, M. 1991], [AARTS, E. et al. 2003]. Ambient Intelligence has potential applications in many areas of life, including home, office, transport, industry, entertainment, tourism, recommender systems, safety systems, healthcare and supported living. Ambient Intelligence will undoubtedly bring substantial economic and social benefits to citizens and industry, but they will come alloyed with many risks.

Ambient Intelligence can be identified as an intelligent, embedded, digital environment that is sensitive and responsive to the presence of people [GAGGIOLI, A. 2005], with five related key technology features: embedded, context aware, personalized, adaptive, and anticipatory [AARTS, E. 2004]. According to these definitions each of the integration of computer technologies in AmI will inevitably open up issues of privacy, risks, acceptance and security. It has been widely acknowledged that is a need for acceptable standards and for laws regulating access, to avoid social and ethical problems [SADRI, F. 2011].

This paper presents a survey of Privacy issues in Ambient Intelligence´s Applications in order to identify the relevant design issues that should be addressed in order to provide privacy in the design of Ambient Intelligence´s applications focused in the user´s domain and involved technologies. This architecture should include several levels of privacy about how a specific Ambient Intelligence's application, acquires, stores, manages, shares and sends different types of personal dates. We propose a conceptual framework that contains a Privacy Management System and a Privacy Enforcement Controller that takes care of the interaction between technologies and devices, users and application´s domain.

The related work is organized as follows: Section 2 presents a survey of the Ambient Intelligence Applications considered the domain and technologies involved. Privacy Issues in Ambient Intelligence and an overview of Privacy Models developed is discussed in section 3. Conceptual framework Design by Privacy in AmI is explained in Section 4. The research paper concludes in Section 5.

2 Survey of Ambient Intelligence Applications

This section reviews research on Ambient Intelligence applications in order to determinate the principal domains in AmI applications and the involved technologies.

The principal domains in AmI applications can be joined in three categories: Public Services/ Commerce and Business/ Leisure and Entertainment, Education, Healthcare and Assisted Living. The technologies employed include several devices as Smart Sensor, Smart Phones, Tablets, Wireless Sensor Network (Wi-Fi, Bluetooth, NFC, RFID, etc.), Internet (Facebook, WhatsApp, Twitter, You Tube, Blogs, Cloud Computing, etc.).

- *Public Services/ Commerce and Business/ Leisure and Entertainment*

The authors of [BELT, S. et al. 2006] showed potential of improvement and development for future NFC services and mobile phone interactions that make it clear where interaction occurs, where feedback is given, and how the flow of interaction takes place. User problems in the interactions with this technology are strongly related to recognizing the availability of services, as interaction capabilities are often hidden.

A framework for a location based mobile Information and Communications Technology (ICT) system for the tourist industry is presented in [BOJEN NIELSEN, L.MA. 2004]. This project is focused on content, information, products and services than can be offered tourists on a mobile platform, typically tablets or smartphones giving the users extra utility value. The solutions are interactive and based on the needs of the customers and the tourist operators. Qualitative feedback is required to improve and develop customized content for mobile tourism services. The lack of this qualitative information about tourist experiences is a path to follow in combination with existing quantitative information. Ethical aspects about collecting customer data through mobile devices in this framework should been clarified.

The automation of baggage management in an airport is presented in [DE VRIES, P. 2008].

The main goal of baggage in an airport is to manage the transport of the luggage via conveyors, carts and planes to right destination. The baggage is tagged at the Check-In, traditionally with barcodes, nowadays more and more with RFID tags. Visibility, security and privacy of baggage events are challenging issues to address.

In [BORREGO-JARABA, F. et al. 2010] an application to tourism in the city of Córdoba is presented. The solution is based in the use of mobile phones provided with Near Field Communications Technology (NFC) and Smart posters spread up along the smart environments offering the users/visitors, in a way easy, intuitive and context-awareness, support for the navigation and localization in urban smart scenarios. The idea proposed in this work is that the user could design its own routes making use of a set of intelligent objects (Smart Posters) augmented by RFID Tags with information about localizations where the tourist could visit.

- *Education*

Mobile learning (m-learning) [HOLZINGER, A. et al. 2005] provides great opportunities to interact with learning materials in different ways while exploring a physical environment both outdoor and indoor. The use of mobile devices like smartphones may expand learning, freeing the user from ties to a particular location. For instance project Explore! [COSTABILE, Maria F. et al. 2008] an m-learning system implementing a game to help middle school students to acquire historical notions while visiting archaeological parks.

- *Healthcare and Assisted Living*

The qualitative study presented by [KANSTRUP, A.M. et al. 2008] contributes to the design of Information Technologies supporting diabetics in their daily live. Most IT designed for diabetics have an exclusive medical focus. Aspects of co-operation (in particular the data transfer between people) is possible with the availability of medical devices and self-management tools with communication possibilities. There exists an endless offer of networking possibilities for diabetics (forums, chats, weblog, video or picture sharing sides). Through these networks people strengthen and encourage each other, sharing their thoughts, problems and fears and also their experiences. Thus, co-operation is the central activity, accompanied by informing, finding and planning. In the design of the MaXi-project an important implication to consider is a sustainable privacy and security that give the user full benefit and control of the data-flow.

Health monitors may be particularly useful for chronically ill people as well as for elderly citizens [JUNG, D. et al. 2005]. Sensors automatically capture health-related data such as heart rate and blood pressure, the location of the person in reference to a room, or the intake of medication. The data needs to be protected from tampering, from external unqualified access, as well as being kept safe for long term storage.

UbiMeds is a mobile application that would allow patients to have easy access to prescription information in a mobile phone platform [SILVA, J.M. et al. 2009]. This mobile application integrates with current Personal Health Record systems to provide automated scheduling, reminders and tracking of prescription drugs intake, including proactive alerts sent to physicians and relatives then the patient fails to adhere to the prescription regime. Privacy issues are important to consider. This is particularly critical on applications where health related information is involved and when they use third party service such a Google Health or Microsoft Vault to store the health records.

GerAmI (Geriatric Ambient Intelligence) is a system based on agents to facility the care of Alzheimer patients [CORCHADO, J.M. et al. 2008]. The system contains ID door readers, ID bracelets for the patients and the nurses, with each bracelet containing an RFID chip, PDAs for nurses, controllable alarms and locks, and wireless access points. The architecture uses a multi-agent structure. The manager and the patient agents run on a central computer and the nurses agents run on mobile devices. The patient agent records the location of the patient hourly and sends the record to a central database.

Building Bridges is a project for social connection to elderly people, their family and friends. It intends to reduce the risk of loneliness and social isolation of them [DOYLE, J. et al. 2010]. The communication device used to connect elderly people with their peers, family and friends is based in a touch screen. Further functionality includes individual or group calls, a (textual) messaging service, and a “tea room” which represents a chat forum. The aim of this study was to examine usage and usability of the device communication device for these purposes.

Most of the studies about Ambient Intelligence applications are focused in the technologies, in some cases in the users and in a few cases in the issues of social and privacy impact of AmI technology in order to provide personalized services. In spite of there is much agreement about concerns over security and the social and ethical implications of Ambient Intelligence (Figure 1).

They are also crystal clear the reasons why Ambient Intelligences gives rise to security concerns: the collection of large amounts of personal data, the long-term persistence and integration of such data and the possibility of, and in fact often the need for, providing easy access to the data in a technological world increasingly complex.

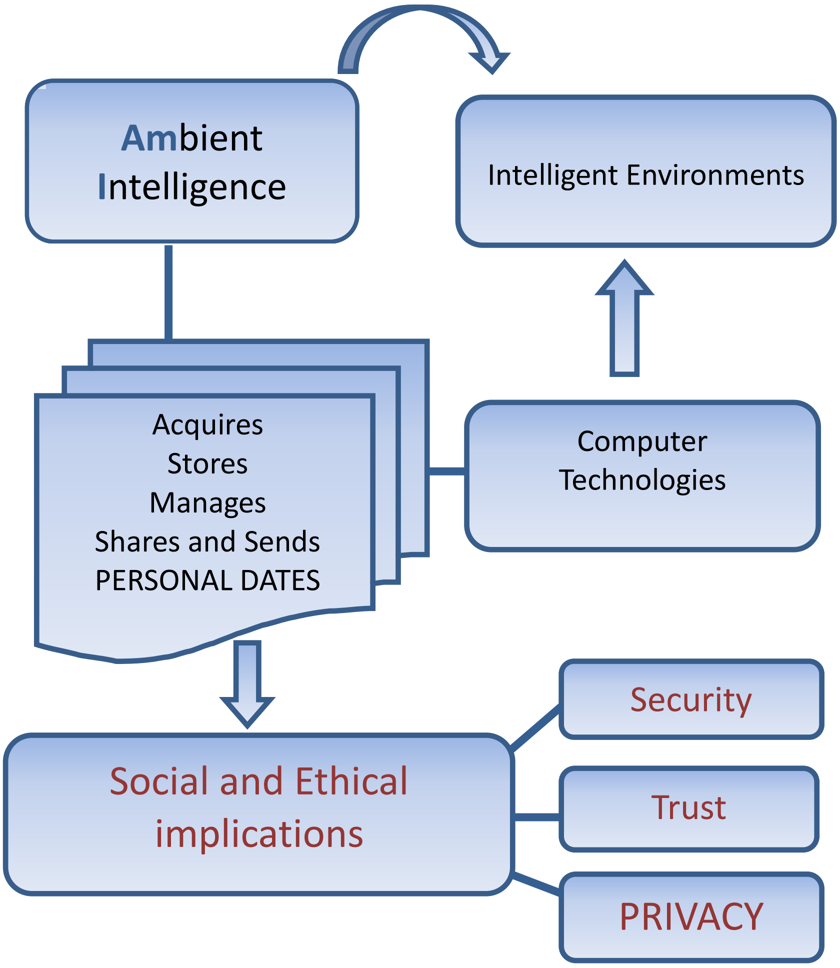

Fig. 1. Privacy in Ambient Intelligence

3 Privacy issues in Ambient Intelligence: Privacy Models

Privacy is a complex, personal, and situation-depending concept that can be interpreted in various ways [BRYCE, C. et al. 2007]. Westin defined privacy as “the claim of an individual to determine what information about himself or herself should be known to others and what uses will be made of it by others” [WESTIN, A.F. 2003]. Privacy is also a human right that is protected by international directives and constitutions. Privacy protection approaches aim at hiding user’s identity and/or some part of the personal identifiable information, whereas privacy management offers transparency to the data subject concerning the collection and processing of personal identifiable information. Privacy and trust are interrelated concepts, that is, “data disclosure means loss of privacy, but an increased level of trustworthiness reduces the need for privacy” [RUOTSALAINEN, PS. Et al. 2012].

Collecting pieces of information from different sources and putting them together to reveal private information is termed as “data fusion” [SWEENEY, L. 2001]. From the data exchanged between applications, the ability to filter identifying information defines “data privacy”. The massive collection of data by the Ambient Intelligence technologies that populate Intelligent Environments enables extensive profiling, which in turn is necessary to deliver the benefits promised by Ambient Intelligence. AmI weaves together heterogeneous systems and devices into a seamless architecture able to accommodate the wishes of commercial agents who want access to as much data from as many sources as possible, not only for a higher level of service personalization, but also of security. 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, more precise are the profiles [DE HERT, P. et al. 2009]. The knowledge derived from the use of AmI can create information asymmetries between those who are under surveillance and those who are doing surveillance.

The development of AmI applications have raised question as what kind of privacy models, services, and architectures offers acceptable level of privacy. Many privacy models developed by researchers are useful in ubiquitous environment.

Existing privacy research in Ambient Intelligence has been mainly focused on achieving awareness and control of information collection and processing. However, many approaches rely on pre-specified privacy policies or assume static or limited scenarios, and do not consider dynamic adaptation of privacy control strategies with respect to changing situations. Yet, privacy regulation is a dynamic and selective process [ALTMAN, I. 1975]. Ambient Intelligence privacy approaches, such as pawS or Confab [LANGHEINRICH, M. 2002], [HONG, J.I. et al. 2004a], provide mechanisms to enhance privacy awareness and control of information collection and processing, but do not directly support users in the privacy configuration process. Privacy of location information has especially attracted considerable research in this area [KRUMM, J. 2009]. Other work focuses on privacy sensitivity of context information [SHEIKH, K. et al. 2008] and privacy-preserving exchange thereof [HESSELMAN, C. et al. 2008].

SWAMI (Safeguards in a World of Ambient Intelligence) [WRIGHT, D. et al. 2008], was a policy-oriented research project focused on social, economic, legal, technological and ethical issues of AmI with particular regard to privacy, trust, security and identity through four dark scenarios that encompass individual-societal and private-public concerns. The results of 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.

The study presented in [FRIEDEWALD, M. et al. 2005], involves more than 70 Research and Development projects, from the point of view of what types of scenario they focus on, what assumptions they do about the users, and the control of AmI systems they envisage. The projects cover five application domains: home, health, shopping, work and mobility, leisure and entertainment. In the envisaged and developing applications, where the AmI system was aimed at providing safety or security it had a high level of control. In particular, AmI control is assumed to be very high in envisaged emergency situations, requiring little numbers of communication with humans. On the other hand, where the system had a more advice-giving role it had lower levels of control, possibly subordinate to the user.

In [BOHN, J. et al. 2004] the authors identifies the two central features of AmI that pose the main challenge to privacy: the ability of AmI systems to collect large and detailed amounts of data about individuals' everyday activities over long periods of time, and the enhanced ability for integrating, searching, and retrieving these large amounts of data. These features are central for one of the key objectives of AmI, which is to provide personalized services. AmI can provide sophisticated support for everyday living, but the information capabilities it may use for this purpose can also potentially provide an invisible and comprehensive surveillance network – walls literally can have ears. The authors identify three additional issues to consider in AmI environment: reliability, delegation of control and social compatibility and acceptance.

In [ROUVROY, A. 2008] the author considers the current European privacy and data protection frameworks and questions if they are applicable and adequate for dealing with the kind of data collection and processing that is at the heart of AmI scenarios and technologies. The European human rights framework incorporates "autonomy in the construction of one's identity", explicitly in the right to privacy. One consequence of this statement, interpreted in courts, is the individual's right to control personal information. The pervasiveness of AmI and the invisibility of data collection and information systems may make it highly unlikely that the individual (the person being observed) will retain control over the data. Furthermore, one objective of AmI systems is learning user profiles in order to respond to human needs, but these needs are being defined increasingly by the systems themselves, and thus by the designers of the systems, and not by the users. The author [ROUVROY, A. 2008] shares with [BOHN, J. et al. 2004] the concern about delegation of control in AmI systems that are likely to be distributed systems in which multiple artificial and human agents collaborate and interact.

Other features of AmI studied concern information flow, its advantages and dangers. AmI massively increases the amounts of detailed personalized data that is collected and stored, and has the potential to make, and indeed in some applications must make, such data easily available. Furthermore, as [BOHN, J. et al. 2004] has also observed, personalization of data and provision of services, can ultimately lead to the control and filtering of what news or information the users see. Some authors [FRIEDEWALD, M. et al. 2005] look at data privacy in Ambient Intelligence settings. Their implemented case study concerns to an organization (a university) collecting information about its members accessing Web sites. The purpose of these data is to enable ranking of Web sites and making recommendations to those with similar interests. However, the malicious use of the data can disclose information about what times, and for how long, someone accessed some given Web sites. To counter this, the proposed solution is that users can specify life-cycle policies on data collected on them.

Various researches attempted to quantify privacy using different metrics. In [REITER, M. et al. 1999] the authors use the size of the anonymity set (all the potential subjects that might have sent/received data) to measure the degree of anonymity. In this approach the authors assume that each sender in the set has an equal probability of sending a message. The study presents in [SERJANTOVE, A. et al. 2002] use entropy to measure the anonymity a system can achieve. In the context of design of privacy preserving data mining algorithms, the authors in [AGRAWAL, D. et al. 2001] use differential entropy to quantify the closeness of an attribute value estimated by an adversarial to its original value.

A model of situational faced is presented in [LEDERER, S. et al. 2003]. In [HONG, J.I. et al. 2004b] the authors propose a model that uses control and feedback, the authors suggest that designers of ubicomp systems should deploy a privacy risk analysis considering social and organizational content. This type of analysis considers: Who are the users? What kind of personal information is being shared? How is personal information collected? The authors suggest after the initial privacy risk analysis designers need to prioritize the findings and develop a privacy risk management record. Privacy risk model helps designers consider the specific group of users, potential risks and benefits, and the type of feedback users will be giving the system. Privacy risk models will help with designing and understanding social issues as trends move towards ubiquitous computing environments.

The model suggested in [FRIEDEWALD, M. et al. 2007] included actors, environment, activity, information flow, control level, and enabling technology. The study presented in [ADAMS, A. et al. 2001] looks at privacy as preferences and constraints, and uses a computer-understandable language for expressing them. The authors in [JIANG, X. et al. 2002] consider an information space model, and the authors in [KAPADIA, A. et al. 2007] apply virtual walls for privacy management. Entropy as measure of privacy level is presented in [DIAZ, C. et al. 2002].

Privacy management model proposed by the authors in [LEDERER, S. et al. 2002] considers a preferred privacy level depends on legislation, market features, norms, technology used, nature of personal information disclosed, contextual features, information sensitive, characteristics of information user, and expected cost-benefit ratio.

4 Conceptual framework Design by Privacy in AmI

The most of AmI applications are focused in the technology involved (sensor devices, device´s communication) and in some cases are focused in the user. We consider that the most important element in AmI applications is the user, and so it must be the application that adapts itself to the user´s profiles, being the privacy one of the most important issues to be considered. Different levels of privacy should be identified and appropriate mechanisms shall be developed to distinguish life-threatening requests from other applications with various security priorities and appropriate privacy-protections measures.

The main dimensions of design by privacy based in the AmI’s domain and centered in user are [CLARKE, R. 1997]:

- *Privacy of personal data* (data or information privacy). Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over their data and its use.
- *Privacy of personal behavior* (media privacy). This relates to all aspects of behavior, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places.
- *Privacy of personal experience*. Individuals gather experience through buying books and newspapers and reading the text and images in them, buying or renting recorder video, conducting conversations with other individuals both in person and on the mobile phone, meeting people in small groups, and attending live and cinema events with larger numbers of people. Until very recently, all of these were ephemeral, none of them generated records, and hence each individual's small-scale experiences, and their consolidated large-scale experience, were not visible to others. During the first decade of the 21st century, reading and viewing activities have migrated to screens, are performed under the control of corporations, and are recorded; most conversations have become 'stored electronic communications', each event is recorded and both 'call records' and content may be retained; many individuals' locations are tracked, and correlations are performed to find out who is co-located with whom and how often; and events tickets are paid for using identified payment instruments. This massive consolidation of

individuals' personal experience is available for exploitation, and is exploited.

In the development on AmI´s Applications an important issue to be added from the beginning of the development process is the privacy. To approach design by privacy, an important challenge to be considered is the development of a framework that include the different privacy policies and how can we fusion them in a specific domain in Ambient Intelligence. In order to enforce privacy according to the different privacy policies and how can we fusion them, we propose a framework (Figure 2) based in the AmI's domain and centered in user, that contain a Privacy Management System and a Privacy Enforcement Controller that takes care of interaction between the technologies and devices, user and the application's domain. In order to control the flow of the information it could be interesting to distinguish information acquisition, representation and exploitation.

- Specific privacy policies of the devices (Policies Smart Applications Devices and Intelligent Sensors).
- Specific privacy policies of the communications (Public key certificates).
- Privacy policies than represent the legal requirements (Digital legal requirements).

Privacy Enforcement Controller should include different steps relating to the privacy policies:

- General considerations and characterization of the Application focused in the User's Domain.
- Definition of Privacy targets.
- Identification of threats of each Privacy target.
- Technical controls to protect against threats.
- Assessment of Risk of Privacy.

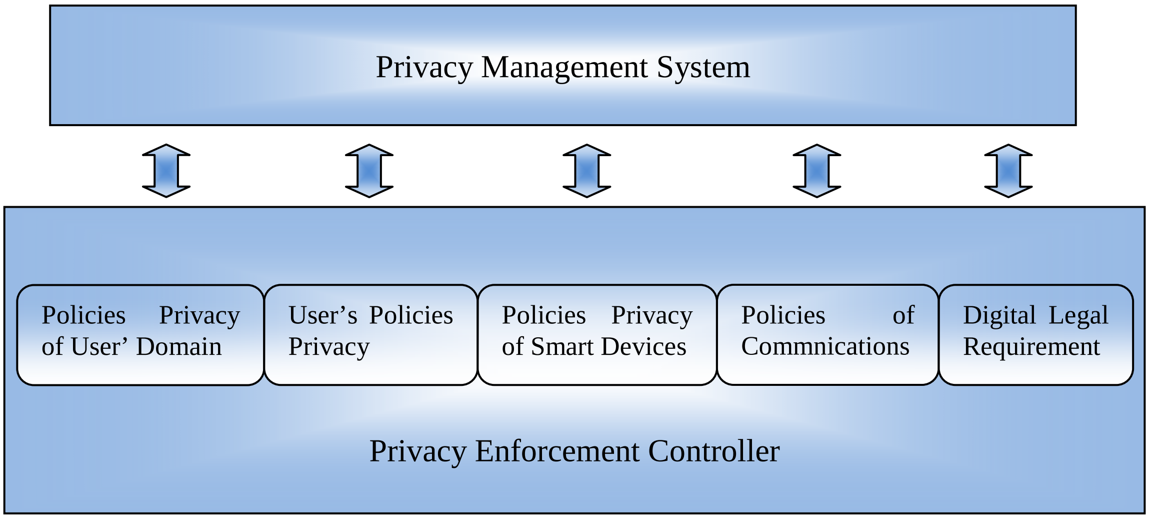
Privacy Management System
Policies Privacy of User' Domain
User's Policies Privacy
Policies Privacy of Smart Devices
Policies of Commnications
Digital Legal Requirement
Privacy Enforcement Controller

Fig. 2. Framework Design by Privacy in Ambient Intelligence

The Privacy Enforcement Controller consists of five different modules:

- Specific privacy policies of the ubiquitous environment (Policies of User's Domain).
- Specific privacy policies of the user (User's Policies Privacy).

This conceptual framework can help to determinate the privacy policies in a specific domain in AmI, that should include several levels of data protection of the rights by the privacy about how a specific Ambient Intelligence's application, acquires, stores, manages, shares and sends different types of personal dates (Table 1).

Table 1. Privacy Policies in Application Domain in AmI

Application´s Domain	General Considerations	User´s conditions	Device´s Characteristics	Communication´s characteristics	Levels of data protection
Healthcare	Healthcare determines the life and death of people. The access to a person's health information can be very important in case of emergency	Patients with autonomous or semi-autonomous life. Patients with limited mental capacity: permanent or transitory (e.g., heart problems and epilepsy)	The character visible or invisible of devices is not so important because there is a Patient Agreement that allows the use of device	The system must be capable of identify to user. Transmission means must grant: Confidentiality, Integrity, Availability of personal data	High
Education	In this domain the public interest consists in the protection of personal data	People interested in enjoy of lifelong learning aim, from any place, at any time and at the individual's own place	The character visible or invisible of the devices is not important because there is an Education Agreement that allows the use of device	The system must be capable of identify to user. Transmissions means must grant: Confidentiality, Integrity, Availability of personal data	Medium
Public Services (Public Transport)	In this domain the public interest consists in the protection of personal data	Public Transport user's	The user must be agreed with the use of geo-localization services includes in devices	The system must be capable of identify to device (it is not mandatory to know the identity of user). Transmissions means must grant: Integrity and Availability of data	Low
Commerce (Tourist/Leisure)	The public interest consists in the protection of personal data (e.g. Prohibits capturing, storing, or reading information from a person's RFID document for particular purpose without that person´s prior knowledge and consent)	Consumers	In this domain could be present invisible devices (e.g. RFID chip)	The system must be capable of identify to person. Transmission means must grant: Integrity and Availability of data	Medium

Table 1. Privacy Policies in Application Domain in AmI

The Privacy Management System should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf; and also plans for responding to incidents and inquiries. The Privacy Management System should be routinely reviewed and updated to ensure that they remain appropriate to the current risk domain. Appropriate safeguards may include: provisions in contracts that address compliance with the data controller's privacy policies and practices; protocols for notifying the data controller in the event of a security breach; employee training and education; provisions for sub-contracting; and a process for conducting audits. The Privacy Management System can also assist in the practical implementation of concepts such "Privacy by Design", whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an afterthought.

The framework Design by Privacy proposed is a step toward proposing design guidelines by privacy for the development of Ambient Intelligence.

5 Conclusions and future work

The Intelligent Environments created by Ambient Intelligence, where users interact in a natural and intuitive way with computational services, collect and process a massive amount of person-related and sensitive information. The AmI´s applications offer great opportunities for people but in many cases, they are too focused on the technology and forgot the people.

The potential uses of personal data have increased tremendously us a result of the wide range of analytics that can provide comprehensive insights into individual's movements, interests, and activities. At the same time, the abundance and persistence of personal data have elevated the risks to individual's privacy; these increased risks signal the needs for more effective safeguards in order to protect privacy. The continuous evolution of social media increases the awareness of privacy issues. Privacy is a complex, personal, and situation-depending concept that can be interpreted in various ways.

Most of the studies about AmI applications are focused in the technologies involved, in some cases in the users and in a few cases in the issues of social and privacy impact of AmI technology in order to provide personalized services. We consider that the most important element in AmI applications is the user, and so it must be the application the one that adapts itself to the user's profiles, being the privacy one of the most important issues to be considered.

This paper presents a survey of AmI applications based in the domains and technologies involved with the aim of to show the awareness of privacy issues in AmI and to identify the relevant design issues that should be addressed in order to provide an architecture that include the different privacy policies that must be considered in the design by privacy in Ambient Intelligence applications. This architecture should include several levels of privacy about how a specific application in AmI acquires, stores, manages, shares and sends different types of personal dates. The privacy models research in Ambient Intelligence has been mainly focused on achieving awareness and control of information collection and processing. Many approaches rely on pre-specified privacy policies or assume static or limited scenarios.

To approach design by privacy, an important challenge to be considered is the development of an architecture that include the different privacy policies and how can we fusion them in a specific domain. To design by privacy we should identify the design issues that should be addressed for his developing.

The conceptual framework proposed contains a Privacy Management System and a Privacy Enforcement Controller that takes care of interaction between technologies and devices, users and application's domain. The Privacy Management System should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf; and also plans for responding to incidents and inquiries. The five modules contained in the Privacy Enforcement Controller should include different steps relating to the privacy policies.

Design by Privacy means that applications should be designed in a way that users know and understand what they are doing and how their personal information will be used. The quality of a system should take in regard several non-technical factors that also play crucial roles in the applications, such as affordability, legal, regulatory and ethical issues like privacy. The quality of the privacy protection highly depends on the used policies. Privacy is already becoming a value to quality for users. Users must understand that they are doing and how their personal information is being used in a specific application.

Our future researches will focus on a methodology to systematically consider privacy issues (PIA, Privacy Impact Assessment) in an AAL System (Ambient Assisted Living) and to implement it in the form of a web application to evaluate its utility. Other lines of researches will focus on the developed of the Privacy Enforcement Controller to the determinate and assessment the different privacy policies in a specific domain in Ambient Intelligence. Design by Privacy in AmI proposed is a step toward proposing design guidelines by privacy for the development of Ambient Intelligence.

6 Acknowledgment

This work has been supported in part by projects: CAM CONTEXTS S2009/TIC-1485, MINECO TEC2012-3783-C02-01.

7 References

[AARTS, E. et al. 2003] AARTS, E. The new everyday: Views of Ambient Intelligence. 010 Publishiers (2003), Rotterdam.

[AARTS, E. 2004] AARTS, E. Ambient intelligence: a multimedia perspective. *IEEE Intelligent Systems. 19*, 1, 12–19.2004.

[ADAMS, A. et al. 2001] ADAMS, A. Privacy in multimedia communications: protection users, not just data. 2001 Presented at: Joint Proceedings of Human-Computer Interaction/Interaction d'Homme-Machine (IMH-HCI 01); 2001; Lille, France p. 49-64.

[AGRAWAL, D. et al. 2001] AGRAWAL, D. "On the design and quantification of privacy preserving data mining algorithms," *Symposium on Principles of Database Systems (PODS´01)*, pp. 247-255, Santa Barbara, May 2001.

[ALTMAN, I. 1975] ALTMAN, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing Company, CA, 1975.

[BELT, S. et al. 2006] BELT, S. (2006-Espoo, Finland), User Perceptions on Mobile Interaction with Visual and RFID Tags. *Proc. of the Workshop on Mobile Interaction with the Real World*, pp. 23-26.

[BOHN, J. et al. 2004] BOHN, J. Living in a world of smart everyday objects-Social, economic, and ethical implications. *Human Ecol. Risk Assess., 10*, 5. 2004.

[BOJEN NIELSEN, L. MA. 2004] BOJEN NIELSEN, L. MA. (2004-Delft, The Netherlands) ICEC'04 Proceedings of the 6th International Conference on Electronic Commerce. Post Disney experience paradigm? Some implications for the development of content to mobile tourist services.

[BORREGO-JARABA, F. et al. 2010] BORREJO-JARABA, F. (2010-Córdoba, Spain). Proceedings of the 23rd International Conference on Industrial Engineering and other Applications of Applied Intelligent Systems. Volume Part III, pp. 229-238 IEA/AIE´10. NFC Solution for the Development of Smart Scenarios Supporting Tourism Applications and Surfing in Urban Environments.

[BRYCE, C. et al. 2007] BRYCE, C. Ubiquitous privacy protection. 2007 Presented at: First IEEE International Workshop on Privacy in Ubiquitous Systems; August 2007; Salzburg, Austria.

[CLARKE, R. 1997] CLARKE, R. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. http://www.rogerclarke.com/DV/Intro.html. 1997.

[CORCHADO, J.M. et al. 2008] CORCHADO, J.M. 2008. GerAmi: improving healthcare delivery in geriatric residences. J. IEEE Intelligent. Systems. (Special Issue on Ambient Intelligence), 3, 2, 19-25.

[COSTABILE, MARIA F. et al. 2008] COSTABILE, MARIA F. CHI'2008 Proceedings-Learning Support. 26th annual SIGCHI conference on Human factors in computing. Explore! Possibilities and Challenges of Mobile Learning.

[DE HERT, P. et al. 2009] DE HERT, P. Pers Ubiquit Comput (2009) 13:435-444. Legal safeguards for privacy and data protection in ambient intelligence. Springer-Verlag London Limited 2008.

[DE VRIES, P. 2008] DE VRIES, P. The state of RFID for e®ective baggage tracking in the airline industry. International Journal of Mobile Communications 2008. 6(2):151{164, 2008.

[DIAZ, C. et al. 2002] DIAZ, C. Towards measuring anonymity. In: Privacy Enhancing Technologies: Second International Workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002: revised papers. New York: Springer-Verlag; 2003:54-68.

[DOYLE, J. et al. 2010] DOYLE, J. (2010-Dundee, UK) BCS´10 Proceedings of the 24th BCS Interaction Specialist Group Conference. Designing a touch screen communication device to support social interaction amongst older adults.

[FRIEDEWALD, M. et al. 2005] FRIEDEWALD, M. Perspectives of ambient intelligence in the home environment. *Telematics Informatics*, *22*, Elsevier, 221–238. 2005.

[FRIEDEWALD, M. et al. 2007] FRIEDEWALD, M. Privacy, identity and security in ambient intelligence: a scenario analysis. Telematics Informatics 2007 Feb;24(1):15-29.

[GAGGIOLI, A. 2005] GAGGIOLI, A. Optimal experience in ambient intelligence. In *Ambient Intelligence*, G. Riva, F. Vatalaro, F. Davide, and M. Alcaniz, Eds., IOS Press, Amsterdam, 35–43. 2005.

[HESSELMAN, C. et al. 2008] HESSELMAN, C. Controlled Disclosure of Context Information across Ubiquitous Computing Domains. In *Intl. Conf. Sensor Networks, Ubiq., and Trustworthy Comp. (SUTC´08)*. IEEE, 2008.

[HOLZINGER, A. et al. 2005] HOLZINGER, A. Lifelong-learning support by mlearning: Example scenarios. *eLearn*, 11 (2005), 2.

[HONG, J.I. et al. 2004a] HONG, J.I. An architecture for privacy-sensitive ubiquitous computing. In *MobySys´0*. ACM, 2004.

[HONG, J.I. et al. 2004b] HONG, J.I. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. *DIS '04 Proceedings of the 5th Conference on Designing Interactive Systems. 91-100. 2004.* http://dx.doi.org/10.1145/1013115.1013129.

[ISTAG, 2001] ISTAG, Scenarios for ambient intelligence in 2010. European Commission Report, http://www.cordis.lu/ist/istag.htm, 2010.

[ISTAG, 2002] ISTAG, Strategic orientation & priorities for IST in FP6. European Commission Report, http://www.cordis.europa.eu/fp7/ict/istag/reports_en.html, 2010.

[ISTAG, 2003] ISTAG, Ambient intelligence: from vision to reality. European Commission Report, http://www.cordis.europa.eu/fp7/ict/istag/reports_en.html, 2010.

[JIANG, X. et al. 2002] JIANG, X. Modeling privacy control in context-aware systems. IEEE Pervasive Computing: 2002 Jul.,1(3):59-63. [doi: 10.1109/MPRV.2002.1037723].

[JUNG, D. et al. 2005] JUNG, D. A mobile alerting system for the support of patients with chronic conditions. In First European Conference on Mobile Government (EURO mGOV), Brighton, UK, pages 264{274, 2005}.

[KANSTRUP, A.M. et al. 2008] KANSTRUP, A.M. (2008-Bloomington,USA) PDC'08 Proceedings of the 10th Anniversary Conference on Participatory Design. Design for More: an Ambient Perspective on Diabetes.

[KAPADIA, A. et al. 2007] KAPADIA, A. Virtual walls: protecting digital privacy in pervasive environments. In LaMarca A, Langheinrich M, Truong KN, editors. Pervasive Computing: 5th International Conference, PERVASIVE 2007, Toronto, Canada, May 13-16, 2007, Proceedings (Lecture Notes in Computer Science/Information… Applications, incl. Internet/Web, and HCI): Verlag Berlin, Heidelberg: Springer-Verlag; 2007:162-179.

[KRUMM, J. 2009] KRUMM, J. A survey of computational location privacy. *Pers. and Ubiquitous Comp.*, 13 (6), 2009.

[LANGHEINRICH, M. 2002] LANGHEINRICH, M. A privacy awareness system for ubiquitous computing environments. In *UbiComp´02*. Springer, 2002.

[LEDERER, S. et al. 2002] LEDERER, S. Report No, UCB/CSD-2-1288. Berkeley, CA, USA: University of California; 2002 Jun. A conceptual model and metaphor of everyday privacy in ubiquitous computing environments.

[LEDERER, S. et al. 2003] LEDERER, S. Report No UCB/CSD-3-1257. Berkeley, CA, USA: University of California; 2003 Jul. Managing personal information disclosure in ubiquitous computing environments.

[REITER, M. et al. 1999] REITER, M. "Crowds: Anonymity for web transactions," *Communications of the ACM*, vol. 42, no 3, pp. 32-48, 1999.

[ROUVROY, A. 2008] ROUVROY, A. Privacy, data protection, and the unprecedented challenges of ambient intelligence. *Studies Ethics, Law, Technol. 2*, 1, Article 3. 2008.

[RUOTSALAINEN, PS. et al. 2012] RUOTSALAINEN, PS. A conceptual framework and principles for trusted pervasive health. J. Med Internet Res 2012 Apr;14(2):e52. [doi: 10.2196/jmir.1972].

[SADRI, F. 2011] SADRI, F. Ambient Intelligence: A Survey. ACM Computing Surveys, Vol. 43, Issue 4, Article 36. 2011.

[SERJANTOVE, A. et al. 2002] SERJANTOVE, A. "Towards an information theoretic metric for anonymity;" in *Proceedings of Workshop on Privacy Enhancing Technologies (PET´02)*, LNCS 2482, Springer-Verlag, 2002.

[SHEIKH, K. et al. 2008] SHEIKH, K. Quality-of-Context and its use for Protecting Privacy in Context Aware Systems. *Journal of Software*, 3(3):83-93, 2008.

[SILVA, J.M. et al. 2009] SILVA, J.M. (2009-Beijing, China). Proceedings of the 1st ACM SIGMM International Workshop on Media Studies and Implementations that help improving access to disabled users: UbiMeds: A mobile application to improve accessibility and support medication adherence.

[SWEENEY, L. 2001] SWEENEY, L. *Computational disclosure control: A primer on data Privacy protection,* Ph. D Thesis, MIT, 2001.

[WEISER, M. 1991] WEISER, M. The computer for the twenty-first century. Scientific Am 265(3):91–104.1991.

[WESTIN, AF. 2003] WESTIN, AF. Social and political dimensions of privacy. J Social Issues 2003 Jun; 59(2):431-453. [doi: 10.1111/1540-4560.00072].

[WRIGHT, D. et al. 2008] WRIGHT, D. (2008) Safeguards in a world of ambient intelligence, Springer Press, Dordrecht, p 291.