This document is published in:

Demazeau, Yves et al. (eds.), 2010. *Trends in Applied Intelligent Systems*: 8th International Conference on Practical Applications of Agents and Multiagent Systems, Springer, pp.631-638.

DOI: 10.1007/978-3-642-12433-4_74

A Legal View of Ambient Assisted Living Developments

J.P. Pedraza, M.A. Patricio, A. De Asís, and J.M. Molina

Abstract. In this paper, a legal approach to Ambient Assisted Living is considered. A general framework for context-aware applications is presented and a general view of legal principles to be considered in this framework. The analysis of a specific application of AAL, developed in a previous work, allows understanding these principles in a real development and the applicability for designing AAL applications.

Keywords: AAL, Context Applications, User Identification, Social Guarantees, Privacy and Human Rights.

1 Introduction

The concept of Ambient Intelligent (AmI) includes the contextual information but expand this concept to the ambient surrounding the people. So, electronic or digital part of the ambience (devices) will often need to act intelligently on behalf of people. It is also associated to a society based on unobtrusive, often invisible interactions amongst people and computer-based services taking place in a global computing environment. Context and context-awareness are central issues to ambient intelligence [1]. AmI has also been recognized as a promising approach to tackle the problems in the domain of Assisted Living [2]. Ambient Assisted Living (AAL) born as an initiative from the European Union to emphasize the importance of addressing the needs of the ageing European population, which is growing every year as [3]. The program intends to extend the time the elderly can live in their home environment by increasing the autonomy of people and assisting them in carrying out their daily activities. Several prototypes encompass the functionalities mentioned above: Rentto et al. [4], in the Wireless Wellness Monitor project, have developed a prototype of a smart home that integrates the context

J.P. Pedraza · A. De Asís
Public Law Department, Universidad Carlos III de Madrid, Colmenarejo, Spain
e-mail: {jpedraza@der-pu,aeasis@der-pu}.uc3m.es

M.A. Patricio · J.M. Molina
Computer Science Department, Universidad Carlos III de Madrid, Colmenarejo, Spain
e-mail: {mpatrici@inf,molina@ia}.uc3m.es

information from health monitoring devices and the information from the home appliances. Becker et al. [5] describe the amiCa project which supports monitoring of daily liquid and food intakes, location tracking and fall detection. The PAUL (Personal Assistant Unit for Living) system from University of Kaiserslautern [6] collects signals from motion detectors, wall switches or body signals, and interprets them to assist the user in his daily life but also to monitor his health condition and to safeguard him. There are also several approaches with a distributed architecture like AMADE [7] that integrates an alert management system as well as automated identification, location and movement control systems.

All these approaches are promising applications from an engineering point of view, but, no legal aspects are considered in the development. Clearly, an important point is the necessity to identify the users of these systems. Two different approaches could be considered, one approach is based in the cooperation of the user to be identified and another one is based in the non-cooperative environment (for example in surveillance applications). Biometric technology has legal implications because it has the potential to reveal much more about a person than just their identity. For instance, retina scans, and other methods, can reveal medical conditions. Thus biometric technology can be a potential threaten to privacy [8]. European and American judges [9] have categorized privacy as taking three distinct forms. These includes [10]: a) physical privacy or freedom from contact with other people; b) decisional privacy or the freedom of the individual to make private choices about the personal and intimate matters that affect her without undue government interference and c) informational privacy or freedom of individual to limit access to certain personal information about oneself. Obviously, biometrical technology is related with the a) and c) issues. Biometric identification, of course, is not a new technology. Introduced more than a century ago, fingerprint technology is perhaps the most common biometric identification technique. Thus the social risk [11] associated to this technology is not new. However, technological advances, among other factors [12], have increased the social risk associated to technique because: a) they have reduced the social tendency to reject its use; b) they have allowed their widespread use [13] and c) they have enabled to obtain more sensitive information on the subject.

In this work, authors review legal consideration in biometric identification to propose a set of legal principles on a general context aware framework. Finally a real application is studied from these principles.

2 Legal Consideration in Biometric User Identification

States and stakeholders should make further efforts to ensure that biometrical applications are monitored and the rights and freedoms of individuals are respected [14]. In particular, they should take into account, inter alia: the legal nature of relations (public or private) and the characteristics of the devices (ability to obtain sensitive information):

a) Private Relations (Private Users and Private Services) [15]. Because most biometric scanning will result from private sector activities where the user voluntarily gives up information, legal privacy concerns will usually be implicated to ensure

informed consent and the transparency with the data subject. This is achieved providing them with the information about the systems and granting the right to access to personal data and, where appropriate, the right to have it deleted or rectified or blocked if they are inaccurate or have been unlawfully processed [16].

b) Public Relations (Private/Public Users and Public Services). In this context, the social guarantees, depends on the particular case and the results of legal test of the "balancing interests" [17][18]. There are common principles to "balancing interest" test: proportionality and reasonableness.

The principle of proportionality requires that measures implemented should be appropriate for attaining the objective pursued and must not go beyond what is necessary to achieve it. The reasonableness of a measure is therefore to be adjudged in the light of the nature and legal consequences of the relevant remedy and of the relevant rights and interests of all the persons concerned.

Also in this field, States shall ensure that appropriate procedures guaranteeing the dignity and privacy of the applicant, in particular, the protection of personal data. The States concerned shall closely monitor the implementation of the social guarantees, including: a) the general information on features and uses of systems; b) all the technical and organizational security measures required to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and all other unlawful forms of processing the personal data; c) the collection and transmission of biometric identifiers; d) any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified; e) in all cases the level of security shall be adapted to the sensitive nature of the data; f) in general, the techniques taken to ensure compliance with data protection provisions and provide a mechanism for citizens to access, control, and verify their information. Society as a whole needs to be aware of the obligations and rights that are applicable in relation to the use of biometric applications. Therefore it makes sense to create a regulatory model for the collection, use and dissemination of biometric information. In that regard, there're several options like laissez faire approach, self-regulation, public regulation [19][20][21]. Under a laissez faire regime, no authority requires businesses to disclose their biometric policies to consumers. Therefore, it would be difficult for customers to comprehensively weigh the alternatives. The self regulation is not sufficient because entails one big drawback: the lack of enforcement. The last alternative deals with binding legislation with effective, proportionate and dissuasive sanctions for infringements.

3 Regulatory Model for AAL Developments

A generic framework of an AAL Application consists of three layers as shown in Figure 1. At the bottom of the Model is the Location/Monitor Layer, which is responsible for processing sensory information received by a collection of

heterogeneous sensors into useful information for Context-Aware services. The set of sensors that monitor the activity of individuals are often organized in so-called sensor networks. With this sensory information, the Context Layer aims to answer the questions previously raised. Therefore, it is necessary to process and model information through the “Physical Context Manager” module. This module, in turn, is able to interact with the sensory layer in order to select certain preferences in the operation of the sensors. An AAL application should adapt its sensory information dynamically to the needs of users, taking into account a wide range of users and situations they may encounter. Through the “Logical Context Manager” module, the system is capable of adapting Context-Aware sensory information based on knowledge about their needs and characteristics, stored in what is called “Personal Profile”. This profile or logical context can be obtained directly through inputs by the user preferences, or by interaction with the environment observed from the sensory system. With the merger of the logical and physical context information, the system is able to obtain the Context-Aware "User Model". The “User Model” plays a critical role in Context-Aware systems, since it embodies, on the one hand, the high-level semantic knowledge of actions of the user received from the sensory system; on the other, the user preferences, as well as its capabilities and limitations. Among these limitations, we may include information on their cognitive and sensorial level, or physical disabilities (for instance, elderly or handicapped people). Finally, once established "User Model", the Context Layer has a "Reasoning System" module capable of inferring and accommodating the needs of services to the final users in the field of a specific Context-Aware application.

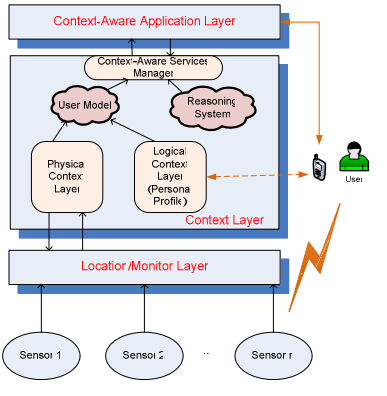

Fig. 1 Abstract Model of Context-Aware Applications

Identification and personalization are essential features of AAL services. The contextual framework needs a biometric scheme with the following features: (a) multibiometric: which combines several sources of biometric information (traits, sensors, etc.) with the aim of mitigating the inherent limitations of each source, obtaining a more reliable and accurate system; (b) highly transparent, highly

accepted, and low intrusive, using biometric traits that can be acquired even without any cooperation of the user (e.g. face, voice) and well socially accepted (like the handwritten signature); (c) able of inferring human activity and analyzing user emotions, therefore significantly focused on services customization. These requirements affect directly to many legal aspects that should the considered before the development of industrial applications, to be used in the private sector or public sector. A generic legal framework of a Context-Aware Application should be composed by principles and fundamental rules, taking into account: (a) Central axiological elements: The protection of human dignity, fundamental rights and in particular the protection of personal data, are the key issues of regulatory model; (b) Principles: This regulatory model and a range of implementing measures needs to be adopted to complete the legal framework, should duly take into account some general principles. From our point of view, the general principles that should be taken into account could resume in the following ones:

1. Public objective driven vs. technology driven: the legal treatment for context-aware applications should not be 'technology-driven', in the sense that the almost limitless opportunities offered by new technologies should always be checked against relevant human rights protection principles and used only insofar as they comply with those principles.
2. Proportionality: requires that measures implemented should be appropriate for attaining the objective pursued and must not go beyond what is necessary to achieve it. The use of biometrics should not in principle be chosen if the objective can also be reached using other, less radical means.
3. Reasonability: reasonableness of a measure is therefore to be adjudged in the light of the nature and legal consequences of the relevant remedy and of the relevant rights and interests of all the persons concerned.
4. Data governance: is a useful principle that covers all legal, technical and organizational means by which organizations ensure full responsibility over the way in which data are handled, such as planning and control, use of sound technology, adequate training of staff, compliance audits, etc.
5. Human rights protection by design: human rights protection requirements should be an integral part of all system development and should not just be seen as a necessary condition for the legality of a system.
6. Best Available Techniques: shall mean the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing in principle the basis for ITS applications and systems to be compliant with Human rights protection requirements.
7. Precautionary: where there is scientific uncertainty as to the existence or extent of risks to human rights, the institutions may take protective measures without having to wait until the reality and seriousness of those risks become fully apparent.
8. Technology neutrality: regulatory framework must be flexible enough to cover all techniques that may be used to provide context-aware applications.

4 An AAL Case of Study

Several AAL developments have been carried out in our laboratory, a complete description could be consulted in [22][23][24]. In these applications, the provisioning of the services occurs automatically in the Context Engine as the right context is found to each user: Role, Zone, Location, etc… For example, a grandmother sitting in a wheelchair with who's carrying a WiFi device and who usually take her medications every day, so the following rule is defined and discovered by the system:

Scenario I: Intelligent Home + Elderly + Taking Medication
Event part: *When Rose Mary, the grandmother of the family, carrying a PDA is detected in the TV room,*
Condition part: *(and) it is the first time in the day,*
Action part: *(then) turn on the device, and send a MEDICATION'S ALERT.*

The following rule is evaluated in order to offer the appropriate services to the elderly woman who is in the TV room. The intelligent home is able to know the location of each person at home (using cameras or wifi), identify each one (using cameras or wifi), correspond each mobile device with people who carry out, and apply context-rules to inform each user. In this simple example, some legal consideration should be done, following the principles of the proposed regulatory model (section 4):

1. Public objective driven vs. technology driven: the device could offer higher level functionalities in an automatic way but considering public goal and "the principle of the independence of will", the device should be configured in order to capture the information defined by the user.
2. Proportionality: the identification system does not need a personal recognition based on cameras only the identification of the device is necessary.
3. Reasonability: in this application the message send to the user could be turn off (other applications need to be always turn on, for example, in a hospital the message should send to medical assistance to be considered in any case).
4. Data governance: the whole system is under personal data privacy law.
5. Human rights protection by design: user should be able to configure the way in which the alarm is showed in order to avoid the publicity of the personal situation to other people at home.
6. Best Available Techniques: the designed devices should consider the minimum effort from the user and a low cost.
7. Precautionary: the technology involved should be tested to avoid healthy problems as to interfere with medical devices.
8. Technology neutrality: the functionalities should be open to any device with similar technology.

These legal principles define the deployment of the system and technology and devices to be used, they impose several requirements on software development and they bring a new way to define AAL applications.

Acknowledgements. This work has been partially supported by Projects CICYT TIN2008-06742-C02-02/TSI, CICYT TEC2008-06732-C02-02/TEC, SINPROB, CAM CONTEXTS S2009/TIC-1485 and DPS2008-07029-C02-02.

References

1. Schmidt, A.: Interactive context-aware systems interacting with ambient intelligence. IOS Press, Amsterdam (2005)
2. Emiliani, P., Stephanidis, C.: Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities. IBM Systems Journal 44(3), 605–619 (2005)
3. World population prospects: The 2006 revision and world urbanization prospects: The revision. Technical report, Population Division of the Department of Economic and Social Affairs of the United Nations Secretariat (last access: February 28, 2009)
4. Rentto, K., Korhonen, I., Vaatanen, A., Pekkarinen, L., Tuomisto, T., Cluitmans, L., Lappalainen, R.: Users' preferences for ubiquitous computing applications at home. In: First European Symposium on Ambient Intelligence 2003, Veldhoven, The Netherlands (2003)
5. Becker, M., Werkman, E., Anastasopoulos, M., Kleinberger, T.: Approaching ambient intelligent home care system. In: Pervasive Health Conference and Workshops 2006, pp. 1–10 (2006)
6. Floeck, M., Litz, L.: Integration of home automation technology into an assisted living concept. Assisted Living Systems-Models, Architectures and Engineering Approaches (2007)
7. Fraile, J., Bajo, J., Corchado, J.: Amade: Developing a multi-agent architecture for home care environments. In: 7th Ibero-American Workshop in Multi-Agent Systems (2008)
8. That right is enshrined in Article 12 of Universal Declaration of Human Rights, Article 7 the Charter of Fundamental Rights of the European Union (2000/C 364/01) and implicity in Fourth Amendment
9. See. European Court of Human Rights, López Ostra v. Spain - 16798/90 [1994] ECHR 46 (December 9, 1994). Katz v. United States, 389 U.S 347 (1967); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989); To see differences between legal systems: Kirtley: Is implementing the EU Data Protection Directive in the United States irreconcilable with the First Amendment? Government Information Quaterly 16(2), 87–91 (2001)
10. Jhon, W.: Biometric scanning, law & policy: identifying the concerns-drafting the biometric blueprint. U. Pitt. L. Rev. 59, 97–155 (1997-1998)
11. Beck, U.: La sociedad del riesgo: hacia una nueva modernidad (1998)
12. Lin, C.H., Liou, D.Y., Wu, K.W.: Opportunities and challenges created by terrorism. Technological Forecasting and Social Change 74(2), 148–164, 158 (2007)
13. Kennedy, G.: Thumbs up for biometric authentication. Computer Law Review & Tech. 8, 379–407 (2003-2004)
14. Parejo Alfonso, Luciano: Seguridad pública y policía administrativa de seguridad, Valencia (2008)
15. To see examples, `http://www.biometrics.gov/Documents/FAQ.pdf` (040809)

16. That rights are enshrined in 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 and on the free movement of such data OJ L 281, pp. 31–50 (23.11.1995) and 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 OJ L 201, pp. 37–47 (31.7.2002) In the United States doesn't exist general regulation for data protection. Kuner, C.: An international legal framework for data protection: issues and prospects. Computer Law & Security Review 25, 307–317 (2009)
17. Haas, E.: Back to the future? The use of biometrics, its impact on airport security, and how this technology should be governed. Journal of Air Law and Commerce (69), 459 (Spring 2004)
18. Rodríguez de Santiago, J.M[a].: La ponderación de bienes e intereses en el Derecho Administrativo, Madrid (2000)
19. Kennedy. Note 20
20. Star, G.: Airport security technology: is the use of biometric identification technology valid under the Fourth Amendment? Law & Technology Journal 251 (2001-2002)
21. Luther, J.: Razonabilidad y dignidad humana. Revista de derecho constitucional europeo 7, 295–326 (2007)
22. Cilla, R., Patricio, M.A., Berlanga, A., García, J., Molina, J.M.: Non-supervised Discovering of User Activities in Visual Sensor Networks for Ambient Intelligence applications. Special session Challenges in Ubiquitous Personal Healthcare and Ambient Assisted Living, ISABEL (2009)
23. Sánchez-Pi, N., Molina, J.M.: A smart solution for elders in ambient assisted living. In: Mira, J., Ferrández, J.M., Álvarez, J.R., de la Paz, F., Toledo, F.J., et al. (eds.) IWINAC 2009, Part II, LNCS, vol. 5602, pp. 95–103. Springer, Heidelberg (2009)
24. Sánchez-Pi, N., Molina, J.M.: A centralized approach to an ambient assisted living application: An intelligent home. In: Omatu, S., Rocha, M.P., Bravo, J., Fernández, F., Corchado, E., Bustillo, A., Corchado, J.M. (eds.) IWANN 2009. LNCS, vol. 5518, pp. 706–709. Springer, Heidelberg (2009); Proceedings of International Workshop on Ambient Assisted Living (IWAAL 2009)