García-Pedrajas, N. et al. (eds.), 2010. *Trends in Applied Intelligent Systems*: 23rd International Conference on Industrial Engineering and Other Applications of Applied Intelligent Systems, IEA/AIE 2010, Cordoba, Spain, June 1-4, 2010, Proceedings, Part I. (Lecture Notes in Artificial Intelligence, 6096) Springer, pp 397-406.
DOI: 10.1007/978-3-642-13022-9_40

A Regulatory Model for Context-Aware Abstract Framework*

Juanita Pedraza[1], Miguel Á. Patricio[2], Agustín De Asís[1], and José M. Molina[2]

[1] Public Law Department
[2] Computer Science Department
Universidad Carlos III de Madrid
Colmenarejo, Spain
jpedraza@der-pu.uc3m.es, mpatrici@inf.uc3m.es,
aeasis@der-pu.uc3m.es, molina@ia.uc3m.es

Abstract. This paper presents a general framework to define a context aware application and analyzes social guarantees to be considered to develop this kind of applications following legal assumptions as privacy, human rights, etc. We present a review of legal issues in biometric user identification where several legal aspects have been developed in European Union regulation and a general framework to define context aware applications. As main result, paper presents a legal framework to be taken into account in any context-based application to ensure a harmonious and coherent system for the protection of fundamental rights.

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

1 Introduction

Nowadays it is increasingly important the development of reliable procedures that allow the secure access to new services, and the univocal identification of the user, key functionality in the scenarios of environmental intelligence and access control. The level of security given by the classic techniques based in the possession of an object (card) or an information (personal number), are surpassed by new techniques that work with measurable personal traits, both anatomic (fingerprints, iris, etc.) and behavioral (gait, key-stroking, etc.). At present, many research efforts are being made in developing new algorithms and techniques that allow to implement multi-biometric systems which combine different biometric traits to obtain a more secure and reliable identification.

Identification and personalization are essential features of context-based services. The development of efficient, non-vulnerable and non-intrusive biometric recognition

* This work was supported in part by Projects CICYT TIN2008-06742-C02-02/TSI, CICYT TEC2008-06732-C02-02/TEC, CAM CONTEXTS (S2009/TIC-1485) and DPS2008-07029-C02-02.

techniques is still an open issue in the biometrics field (in which, however, enormous scientific contributions have been made over the last decade). It is also a necessity to obtain contextual systems able to provide a satisfactory user experience.

The Biometric identification must be robust, efficient and quick process to be accepted in strong requirements of security in this networked society [1]. Biometrics aims to recognize a person through the physiological or behavioural attributes [2], such as iris, retina, fingerprints, DNA and so on. The cause for this increment in research fields is the security sector and the possible application in many its aspects, such as video-surveillance or access control.

The new proposals aim to approach Biometrics Recognition in an innovative manner, providing technological solutions which remove their current limitations, and integrating Biometrics Recognition in context inference and fusion activities. The contextual framework needs a biometric scheme with the following features:

- 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.
- 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)
- 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.

In this work, authors define a set of procedures that should be contained in the context-aware applications to accomplish the legal aspect in Europe and USA related to privacy and human rights. Section 2 is center in a description of the e-passport and legal problems that surround it. In section 3, we present a general model to represent context-aware applications. A description of the legal issues to be considered in context-aware applications is enumerated in section 4. Finally, in section 5 some conclusions are included.

2 A Case Study of Legal Aspects in User Identification: E-Passports

A passport traditionally has three security requirements: (1) authenticity and integrity of the document (and its data), (2) match with the holder, and (3) authorization, depending on the situation of use. These requirements had been hardened, among other reasons, as a result of 9/11 attacks and the bombings in Madrid and London: the US, for instance, required that countries that wished to continue to participate in the visa waiver program need to provide their citizens with machine readable travel documents (MRTDs) with digital photographs.

The machine readable character of these biometric passports will be made by integrating a contactless chip into the document. The standards have been developed within the International Civil Aviation Organization (ICAO). ICAO has selected the face as biometric because it is simple to obtain, in a relatively non-intrusive manner, and is already widely used.

The EU requires an additional protection mechanism for fingerprints in accordance with the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

The principle of proportionality is a cornerstone of this legal norm: the biometric features in passports and travel documents shall only be used for verifying: (a) the authenticity of the document; (b) the identity of the holder by means of directly available comparable features when the passport or other travel documents are required to be produced by law [3].

However, this principle is insufficient: this regulation, in the light of the European data protection directive [4], has other critical subjects to consider, for instance [5][6]:

(1) Clear and legitimate objectives: the biometric data should not be processed further than for a specific and lawful purpose: if data are needed for a specific and legitimate purpose they can be used; if they are not needed for a well-defined purpose, personal data should not be used,

(2) Security: the process should be accurate and data should not be kept longer than necessary; the handling of relevant data should be done in a secure way, and the data should not be transferred to those countries that do not ensure data protection,

(3) Citizens rights: the procedures should be in accordance with data subject's rights.

Additionally, biometric technology can be a potential threaten to dignity and other human rights; especially those that are leading us towards the ubiquitous Information Society, like context-aware applications, present fundamental challenges to notions of human rights, privacy and trust, especially in a context where governments need appropriate instruments to guarantee the security of the citizen, but they have to fully respect the citizen's fundamental rights.

3 Context Aware Applications: An Abstract Model

The more widely accepted and used definition of what context is, and it was given by Dey [7] where he defines context as: “any information that characterizes a situation related to the interaction between humans, applications, and the surrounding environment.” There are many developing systems such as platforms, frameworks and applications for offering context-aware services. The Context Toolkit proposed in [7] assist for instance developers by providing them with abstractions to build context-aware applications. The Context Fusion Networks [8] allows context-aware applications to select distributed data sources and compose them. The Context Fabric [9] is another toolkit which facilitates the development of privacy-sensitive, ubiquitous computing applications. There are previous approaches like Entree [10] which uses a knowledge base and case-based reasoning to recommend restaurant or for instance Cyberguide [11] project which provides user with context-aware information about the projects performed at GVU center in Atlanta with TV remote controllers throughout the building to detect users locations and provide them with a map that highlights the project demos available in the neighboring area of the user. A recent one is Appear which is a context-aware platform designed to provide contextual information to users in particular and well defined domains. It has a modular architecture and we have already used it in a previous work [12].

In Europe, 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 [13]. AmI has also been recognized as a promising approach to tackle the problems in the domain of Assisted Living [14]. 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 [15]. 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. Moreover, several prototypes encompass the functionalities mentioned above: Rentto et al. [16], in the Wireless Wellness Monitor project, have developed a prototype of a smart home that integrates the context information from health monitoring devices and the information from the home appliances. Becker et al. [17] 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 [18] 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. The data is interpreted using fuzzy logic, automata, pattern recognition and neural networks. It is a good example of the application of artificial intelligence to create proactive assistive environments. There are also several approaches with a distributed architecture like AMADE [19] 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 off 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).

A generic framework of a Context-Aware Application consists of three layers as shown in Figure 1.

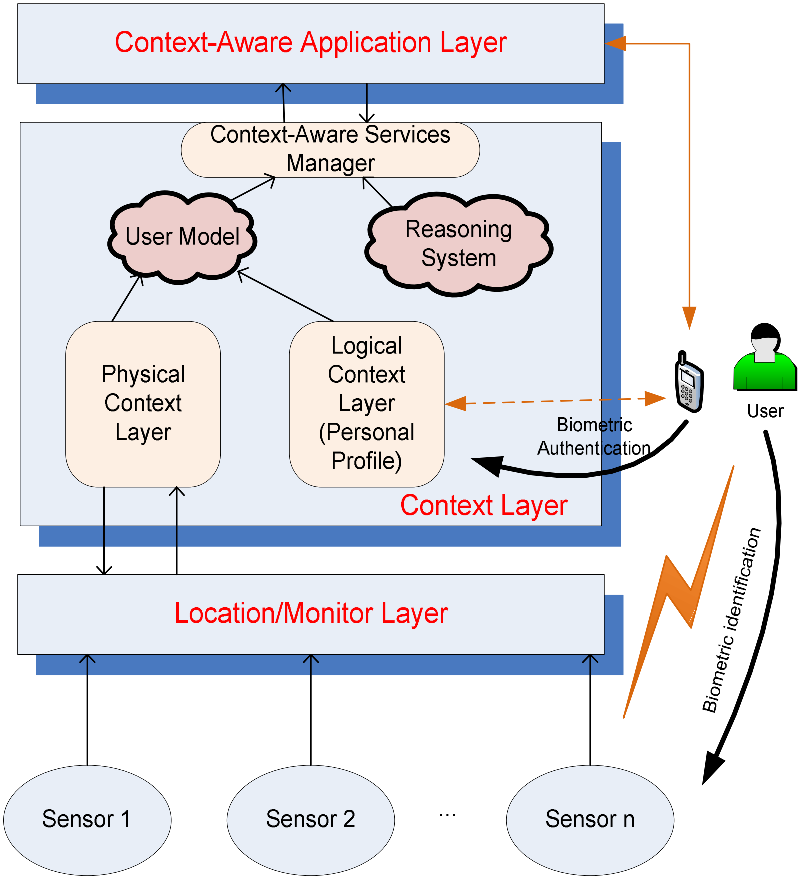

Fig. 1. Abstract Model of Context-Aware Applications

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. The main role of the sensor networks in a Context-Aware environment are to provide to the Context-Aware services the answers to the following questions:

- *Who?* - Information on identifying individuals and objects of interest (animals, vehicles, etc.), i.e., the actors who are in a given scenario. One important aspect of this kind of information is the “Biometric Identification”. By automatic biometric identification systems, we mean those systems that rely on physical characteristics that are unique to each person to ascertain the identification of an individual.

- *Where and When?* - To provide a temporal framework of the action taken and its spatial location, to help to the establishment of the associations between objects and actors.
- *What?* - Information to help the recognition of activities, and the discovery of space-time relations between actors and objects.
- *Why?* - Provide information to discover associations in a particular action in a higher space-time level, in order to uncover plans and behavioral patterns.

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.

A Context-Aware 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. Obviously, in order to update the “Personal Profile”, the system must verify that the user is who he claims to be. In this sense, “Biometric Authentication” is the hardest authentication mechanism to forge.

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.

4 A Regulatory Model for the Use of Context-Aware Applications

Society as a whole needs to be aware of the obligations and rights those are applicable in relation to the use of context-aware applications. Therefore it makes sense to create a regulatory model for the use of context-aware applications [20][21][22][23].

A generic legal framework of a Context-Aware Application should be composed by principles and fundamental rules as shown in Figure 2.

This model should duly take 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.

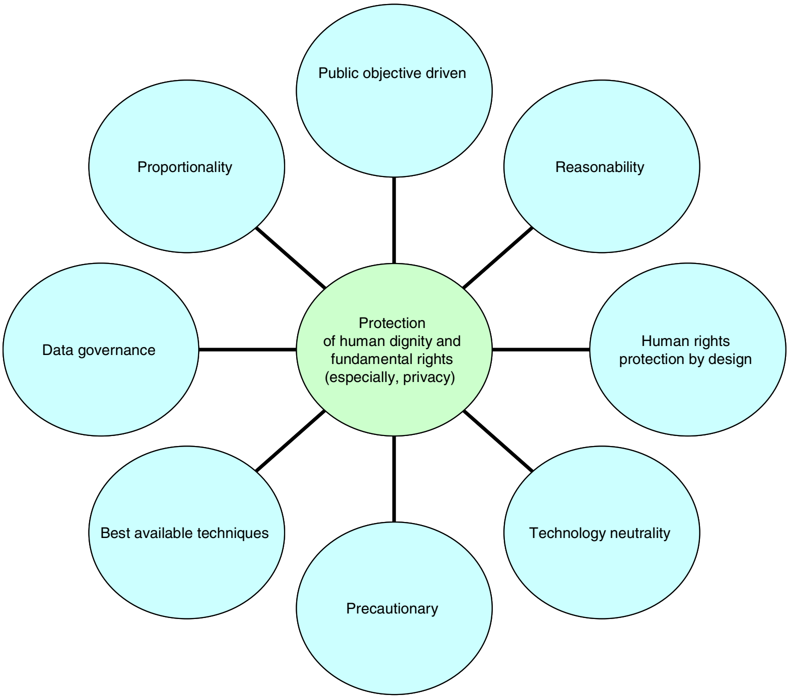

Fig. 2. Generic Legal Framework of a Context-Aware Application

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 [24].
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. [24]
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 [24].
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 [24].
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.

These principles should be considered in context aware applications to include legal requirements in analysis and design phases of software development, and, at the same time, national and international regulations should consider the new capacities of technology applied in these kind of systems.

5 Conclusions

In this paper, we present the necessity to consider legal aspect, related with privacy or human rights, into the development of the incipient context based services. Clearly, context based services and Ambient Intelligence (and the most promising work area in Europe that is Ambient Assisted Living, ALL) needs a great effort in research new identification procedures. These new procedures should be non-intrusive, non-cooperative, in order to the user be immersed in an Intelligent Environment that knows who is, where is and his/her preferences. These new paradigms should be development accomplished the legal issues to allow users be citizen maintaining their legal rights.

References

1. Jain, A.K., Bolle, R.M., Pankanti, S.: Biometrics: Personal Identification in a Net-worked Society. Kluwer, Norwell (1999)
2. Daugman, J.: Biometric Decision Landscape, Technique Report No. TR482, University of Cambridge Computer Laboratory (1999)
3. Schouten, B., Jacobs, B.: Biometrics and their use in e-passports. Image and Vision Computing 27, 305–312 (2009)

4. Directive 95/46/EC of the European Parliament and of the Council of October 24, 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, 23.11.1995, p. 31–50 and Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002, p. 37–47
5. Wrighta, D., Gutwirthb, S., Friedewaldc, M., De Hertb, P., Langheinrichd, M., Moscibrodab, A.: Privacy, trust and policy-making: Challenges and responses. Computer law & security review 25, 69–83 (2009)
6. Grijpink, J.: Biometrics and Privacy. Computer Law & Security Report 17(3) (2001)
7. Dey, A.K., Saber, D., Abowd, G.D.: A conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications. Human-Computer Interaction (HCI) Journal 16, 97–166 (2001)
8. Chen, G., Kotz, D.: Context Aggregation and Dissemination in Ubiquitous Computing Systems. In: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, June 20-21, 2002, p. 105 (2002)
9. Hong, J.: The context fabric: An infrastructure for context-aware computing. In: Minneapolis, A.P. (ed.) Extended Abstracts of ACM Conference on Human Factors in Computing Systems (CHI 2002), pp. 554–555. ACM Press, Minneapolis (2002)
10. Burke, R., Hammond, K., Young, B.: Knowledge-based navigation of complex information spaces. In: Proceedings of the National Conference on Artificial Intelligence, pp. 462–468 (1996)
11. Abowd, G., Atkeson, C., Hong, J., Long, S., Kooper, R., Pinkerton, M.: Cyber-guide: A mobile context-aware tour guide. Wireless Networks 3(5), 421–433 (1997)
12. Sanchez-Pi, N., Fuentes, V., Carbo, J., Molina, J.: Knowledge-based system to define context in commercial applications. In: Proceedings of 8th International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD), Qingdao, China (2007)
13. Schmidt, A.: Interactive context-aware systems interacting with ambient intelligence. IOS Press, Amsterdam (2005)
14. 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)
15. 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 Saturday, February 28, 2009; 12:01:46 AM) (2006)
16. 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)
17. 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)
18. Floeck, M., Litz, L.: Integration of home automation technology into an assisted living concept. Assisted Living Systems-Models, Architectures and Engineering Approaches (2007)
19. 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)

20. 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), 459y ss (spring 2004)
21. Star, G.: Airport security technology: is the use of biometric identification technology valid under the Fourth Amendment? Law & Technology Journal (251) (2001-2002)
22. Luther, J.: Razonabilidad y dignidad humana. Revista de derecho constitucional europeo (7), 295–326 (2007)
23. Rodríguez de Santiago, J.M^a.: La ponderación de bienes e intereses en el Derecho Administrativo. Madrid (2000)
24. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen (2009/C 276/02) OJC 276/8 (November 17, 2009)