Privacy and Legal Requirements for Developing Biometric Identification Software in Context-Based Applications

Juanita Pedraza[1], Miguel A. 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,aeasis}@der-pu.uc3m.es, mpatrici@inf.uc3m.es, molina@ia.uc3m.es

Abstract

Biometric identification in context-based applications is a promising research area. However, several legal issues should be taken into account when developing context-based applications conforming to legal notions like privacy, human rights, etc. In this paper, we present a guide to the social guarantees to be built into context-based systems for private relations (between private user and private services) and public relations (between private/public users and public services). The proposal in this paper focuses on a set of goals that context-based applications should achieve to guarantee privacy and human rights.

Keywords: *Context-Based Applications, Biometrics Identification, Social Guarantees, Privacy and Human Rights*

1. Introduction

Systems based on the concept of *context-aware computing* have been developed with the intention of transforming the way people interact with new, increasingly smaller and smarter technologies. Context-aware computing was first defined by Shilit [1] who claimed that the main components of context were close at hand. What he was referring to were who you are, what you are doing, where you are, when and why. The information in response to such questions was divided into different categories containing concepts like location, time, space, device type, meteorological conditions, user activity, nearby people or devices, etc. There is also a more widely accepted and used definition of what context is, given by Dey [2]. Dey defines context as “any information that characterizes a situation related to the interaction between humans, applications, and the surrounding environment.”

There are several, such as platforms, frameworks and applications, systems offering context-aware services under development. For instance, the Context Toolkit proposed in [2] assists developers by providing them with abstractions to build context-aware applications. Context Fusion Networks [3] enable context-aware applications to select and compose distributed data sources. Context Fabric [4] is another toolkit that facilitates the development of privacy-sensitive, ubiquitous computing applications. There are earlier approaches, like Entree [5], which uses a knowledge base and case-based reasoning to recommend a restaurant, or the Cyberguide [6] project, which provides users with context-aware information about the projects performed at the GVU center in Atlanta with TV remote controllers throughout the building to detect user locations and provide them with a map that highlights the project demos available in the area in the neighborhood of the user. A recent application is Appear. Appear is a context-aware platform designed to provide contextual information to users in particular and well-defined domains. It has a modular architecture, and it has already been used elsewhere [7].

In Europe, the concept of ambient intelligence (AmI) includes contextual information but expands this concept to people's surroundings. Consequently, the electronic or digital part of the ambience (devices) will often need to act intelligently on behalf of people. It is also associated with 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 in ambient intelligence [8]. AmI has also been recognized as a promising approach for tackling the problems in the assisted living domain [9]. Ambient assisted living (AAL) kicked off as a European Union initiative to emphasize the importance of addressing the needs of the ageing European population, which is growing every year [10]. The program intends to extend the time the elderly can live in their own home environment by increasing the autonomy of people and assisting them in carrying out their daily activities.

There have been several attempts at developing AAL systems. For example, Kang et al. [11] propose a wearable sensor system that measures a person's biofunctions (heart rate, blood pressure, body temperature, body mass index, etc) to provide remote health monitoring and health self-checks at home. Korel and Kao [12] also monitor and combine the vital signs with other context information, such as room temperature or a person's condition in order to detect alarming physical states and prevent health risks in time. Baek et al. [13] have designed an intelligent home care system based on a sensor platform to acquire data on heat and illumination. Taking into account the user's position, the home appliance control system manages the optimal performance of home appliances (such as air conditioner, heater, lights, etc.). Lee et al. [14] implement a bundle of context-aware home services, ranging from doorbell answering services, seamless transfer of the TV image from one display device to another, reminders to turn off appliances after use while cooking or recipe outlines on a nearby display. Healthcare and personal status monitoring applications are also common applications in automated healthcare systems (AHCS); they usually involve the target user wearing sensors, and their main objective is to anticipate or detect health risks.

Furthermore, other systems aim at providing special care to a group of people with some disability. For example, Helal et al. have developed a mobile patient caregiver assistant deployed on a smart phone and responsible for attracting the attention of people with Alzheimer's disease and notifying them about the next action they have to take. Medication prompting functionalities are also frequent in AHCS. For example, Agarawala et al. have developed hardware to facilitate medication at home [15]

Additionally, several prototypes address the above functionalities. As part of the Wireless Wellness Monitor project, Rentto et al. [16] have developed a prototype smart home that integrates the context information from health monitoring devices and the information from home appliances. Becker et al. [17] describe the amiCa project which supports daily liquid and food intake monitoring, location tracking and fall detection. The PAUL (Personal Assistant Unit for Living) system from the University of Kaiserslautern [18] collects and interprets signals from motion detectors, wall switches or body signals to assist users in their daily life but also to monitor and safeguard their health status. The data is interpreted using fuzzy logic, automata, pattern recognition and neural networks. This 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 of view, but no legal issues were considered in their development. Clearly, an important point is the need to identify system users. There are two possible approaches. One approach is based on the cooperation of the user to be identified, and the other is based on the non-cooperative environment (for example, in surveillance applications).

In this paper, we define a set of procedures that context-aware applications should contain to conform to the legal regulations related to privacy and human rights in Europe and the USA. Section 2 focuses on biometric identification techniques, analyzing several alternatives and the need for user cooperation. Section 3 gives an overview of the legal regulations in Europe and USA to illustrate the main points to be taken into account. Section 4 gives a description of the requirements that context-aware applications should meet. Finally, some conclusions are included in Section 5.

2. Context-Aware Applications and Biometric Identification

Nowadays, the development of reliable procedures enabling secure access to new services, and univocal user identification, a key functionality in ambient intelligence and access control scenarios, is increasingly important. The level of security provided by traditional techniques based on object (card) or information (personal number) holdership, are surpassed by new techniques that work with measurable anatomic (fingerprints, iris, etc.) and behavioral (gait, key-stroking, etc.) personal traits. At present, many research efforts focus on developing new algorithms and techniques for implementing multi-biometric systems that combine different biometric traits to obtain a more secure and reliable identification.

On the other hand, crisis management situations result in scenarios where security and univocal identification are of the utmost importance and where the availability of contextual services can notably improve the final results. These scenarios have very particular conditions that represent big technical challenges. For example, a system for the management and coordination of firefighter actions or for medical response in the event of natural disasters must have robust communications across ad hoc networks, distributed positioning algorithms, portable interfaces, context sharing in dynamic networks, decision supporting techniques, automatic identification systems, sensor networks, etc. In the recent past, there have been some trial developments of contextual services in this field, although it is not one of the most studied application areas. An example of these initiatives is Siren, a peer-to-peer contextual computational system that compiles, integrates and distributes the contextual data (basically environmental parameters) in fire scenarios. WIISARD is a system supporting medical response in natural disasters, designed to prevent any possible errors caused by shortages of information.

Identification and personalization are key features of context-based services. The development of efficient, non-vulnerable and non-intrusive biometric recognition techniques is still an open issue in the biometrics field (where, however, enormous scientific progress has been made over the last decade). Contextual systems should also be able to provide a satisfactory user experience.

Reliable biometric systems have long been an attractive goal. John Daugmann from the University of Cambridge describes the reliability of biometric systems as a pattern recognition problem, where the key issue is the relation between interclass and intraclass variability: objects can be reliably classified only if the variation between different instances of a given class is less than the variation between different classes. In face recognition, for example, difficulties arise from the fact that the face is a changeable social organ displaying a variety of expressions, as well as being an active three-dimensional (3D) object whose image varies with viewing angle, pose, illumination, accoutrements, and age. It has been shown that for images taken at least 1 year apart, even today's best algorithms can have error rates of 43% to 50%. Interclass variation is limited compared this intraclass (same face) variation, because different faces possess the same basic set of features in the same canonical geometry.

Biometric identification must be a robust, efficient and quick to process to comply with the strict security requirements in today's networked society [20]. Biometrics aims to recognize a person through physiological or behavioral attributes [21], such as iris, retina, fingerprints, DNA and so on. The security sector and possible applications in many fields, such as video-surveillance or access control, is the main drive behind this growth in research fields. Table 1 summarizes identification procedures, where the classical concepts of verification, identification, false positive, false negative, intrusiveness and cost are compared across several classical biometric techniques.

Table 1. Comparison of several Biometric Identification Procedures

Biometric Technique	Verify	Identify	False Positive	False Negative	Intrusiveness	Cost
Face recognition (2D)	Yes	No	Hard	Easy	Very Low	Low
Fingerprint	Yes	Yes	Very Hard	Very Hard	Medium	Low
Hand geometry	Yes	No	Very Hard	Medium	Low	Medium
Iris Scanning	Yes	Yes	Very Hard	Very Hard	Medium	High
Retinal Scanning	Yes	Yes	Very Hard	Very Hard	High	High
Voice Recognition	Some	No	Medium	Easy	Very Low	Low
Signature	Some	No	Medium	Easy	Low	Medium

The new proposals aim to approach biometrics recognition in an innovative manner, providing technological solutions that overcome their current limitations, and integrating biometrics recognition into context inference and fusion activities. They will integrate human body images acquisition technology using radiation in non-visible ranges (from the S to the millimeter wave band and beyond). Arrays of antennas allowing spatial scanning (probably based on beam turn) will need to be developed for this application. The contextual framework needs a biometric scheme with the following features:

- Multi-biometric: combining several sources of biometric information (traits, sensors, etc.) with the aim of mitigating the inherent limitations of each source and assuring a more reliable and accurate system.

- Highly transparent, highly accepted, and not very intrusive, using biometric traits that can be acquired even without any cooperation from the user (e.g. face, voice) and that are socially well accepted (like the handwritten signature).
- Capable of inferring human activity and analyzing user emotions, therefore significantly focused on services customization.

These requirements directly affect many legal issues that should be considered before developing industrial applications to be used in the private or public sectors.

3. Legal Issues in Biometric Identification

Biometric technology has legal implications because it has the potential of revealing a lot more about a person than just their identity. For instance, retina scans, and other methods, can reveal medical conditions. Thus biometric technology can pose a potential threat to privacy [22].

European and American judges [23] have categorized privacy as taking three distinct forms. These include [24]:

a) Physical privacy or freedom from contact with other people.

b) Decisional privacy or the freedom of individuals to make private choices about the personal and intimate matters concerning them without undue government interference.

c) Informational privacy or freedom of individuals to limit access to certain personal information about themselves. Obviously, biometrical technology is related to issues a) and c).

Biometric identification is, of course, not a new technology. Introduced more than a century ago, fingerprint technology is perhaps the most common biometric identification technique. Thus the social risk [25] associated with this technology is not new [26].

However, technological advances, among other factors [27], have increased the social risk associated with the technique, because: a) they have reduced the social objective to reject its use; b) they have propitiated its widespread use [28], and c) they have enabled more sensitive information to be gathered about the subject.

States and stakeholders should make further efforts to ensure that biometrical applications are monitored and the rights and freedoms of individuals are respected [29]. In particular, they should take into account: the legal nature of relations (public or private) and the characteristics of the devices (ability to gather sensitive information):

a) Private relations (private users and private services) [30]. Because most biometric scanning will result from private sector activities where the user voluntarily surrenders information, legal privacy concerns will usually imply ensuring informed consent is given and transparency for data subjects. This is achieved by providing them with information about the systems and granting the right to access personal data and, where appropriate, the right to have it deleted or rectified or blocked if they are inaccurate or have been unlawfully processed [31].

b) Public relations (private/public users and public services). In this context, the social guarantees depend on the particular case and the results of the balancing test of interests [32][33][34][35]. The balancing test has common principles: proportionality and reasonableness.

The principle of proportionality requires that the implemented measures should be appropriate for attaining and must not go beyond what is necessary to achieve the pursued objective.

The reasonableness of a measure is therefore to be adjudged in the light of the nature and legal consequences of the respective remedy and of the respective rights and interests of all the persons concerned.

Also in this field, states shall ensure that appropriate procedures are set up to guarantee the applicants' dignity and privacy, in particular, the protection of personal data. The states concerned shall closely monitor the implementation of social guarantees, including:

a) general information on system features and uses;

b) all the technical and organizational security measures required to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and all other unlawful forms of processing 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 data collection; 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) generally, the techniques should 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 [32][33][34][35].

In that regard, there are several options like the *laissez-faire* approach, self-regulation, and public regulation [36]. 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 up the alternatives. Self regulation is not sufficient because it has one big drawback: non-enforcement. The last alternative is to provide binding legislation with effective, proportionate and dissuasive sanctions for infringements.

4. Development of Context Applications with Social Guarantees

As a complementary means of a public regulation, the software development industry could, of its own accord or at the government's initiative, introduce some social guarantees in the design of context-based applications, as discussed in the previous section. These social guarantees should be introduced, especially, where there is non-cooperative biometric identification, in order to safeguard users' privacy and human rights. Many legal requirements could be easily built into the context-based applications if they were considered in the analysis and design phase.

From the point of view of the development of context applications, all systems should satisfy the requirements of the Tables 2 and 3. In a software engineering project, each requirement has an identifier, a description of the requirement, a need, a priority and a stability. Need states whether or not the requirement to which the need refers is essential. Stability indicates whether or not the requirement can be modified. As in a classical user requirements document, we have described three types of priorities:

Priority 1: The system must have this requirement.

Priority 2: The system should have this requirement.

Priority 3: The system could have this requirement.

Which are the facilities to be included in context-based system to be used between user and companies? In this case, applications should account for the requirements listed in Table 2.

Table 2. User requirements in context-based systems to be used between users and private companies

ID	Description	Need	Prio.	Stability
URC01	Users must be acquainted with the technical features and the application output, as well as the use to which the company could put these outputs.	Yes	1	Stable
URC02	Users must give their express consent.	Yes	1	Stable
URC03	Users could revoke their express consent at any time.	Yes	1	Stable
URC04	Users should be able to exercise all the rights integrated in the personal data protection legal systems [37].	Yes	1	Stable
URC05	The stored and processed data should conform to the legal regulations on security.	Yes	1	Stable

Which are the facilities to be included in the context-based system to be used between users and government applications? In this case, applications should account for the additional requirements listed in Table 3.

Table 3. Additional user requirements in context-based systems to be used between users and government applications

ID	Description	Need	Prio.	Stability
URC01	Application development should respect the general principles of reasonableness and proportionality.	Yes	1	Stable

ID	Description	Need	Prio.	Stability
URC02	Users receive information about the technical features, the application outputs and the use of these outputs.	Yes	1	Stable
URC03	The application should respect, in any case, users' personal dignity.	Yes	1	Stable
URC04	Users could exercise their rights to protection of personal public data files.	Yes	1	Stable
URC05	Stored and the processed data should conform to the legal regulations on security.	Yes	1	Stable

Finally, the social guarantees system must verify compliance with these requirements, irrespective of the source of the requirements: public regulations or self-regulation process. These requirements should be verified prior to the commercialization or distribution under a software/hardware license or authorization. Liability should cover the developer, the distributer and the user. This subjective scope of liability, plus sanctions (criminal or administrative), is the last part of a legal system for monitoring compliance with social guarantees demanded by the widespread use of these techniques.

5. Conclusions

In this paper, we discussed the need to consider legal issues, related to privacy or human rights, in the development of emerging context-based services. Clearly, context-based services and ambient intelligence (and the most promising work area in Europe, that is, ambient assisted living, ALL) imply a major research effort on new identification procedures. These new procedures should be non-intrusive and non-cooperative, enabling users be immersed in an intelligent environment that knows who they, where they are and their preferences. These new paradigms should be developed to comply with the legal issues and enable users as citizens to retain their legal rights.

Acknowledgements

This work was supported in part by Projects CICYT TIN2008-06742-C02-02/TSI, CICYT TEC2008-06732-C02-02/TEC, SINPROB, CAM MADRINET S-0505/TIC/0255 and DPS2008-07029-C02-02.

References

[1] Shilit, B.N.: A Context-Aware System Architecture for Mobile Distributed Computing. Ph.D thesis, Dept of Computer Science, Columbia University (1995)

[2] 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)

[3] Chen, Guanling, Kotz, David.: 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)

[4] 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)

[5] Burke, R., Hammond, K., Young, B.: Knowledge-based navigation of complex information spaces. In: PROCEEDINGS OF THE NATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE. (1996) 462:468.

[6] Abowd, G., Atkeson, C., Hong, J., Long, S., Kooper, R., Pinkerton, M.: Cyber-guide: A mobile context-aware tour guide. Wireless Networks 3(5) (1997) 421:433

[7] 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)

[8] Schmidt, A.: Interactive context-aware systems interacting with ambient intelligence. IOS Press, Amsterdam (2005)

[9] 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)

[10] 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)

[11] Kang, D., Lee, H., Ko, E., Kang, K., Lee, J.: A wearable context aware system for ubiquitous healthcare. In: 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS 2006, pp. 5192–5195 (2006)

[12] Korel, B.T., Kao, S.: Addressing context awareness techniques in body sensor networks. In: 21st International Conference on Advanced Information Networking and Applications Workshops 2007, pp. 798–803 (2007)

[13] Baek, S.H., Choi, E.C., Huh, J.D.: Design of information management model for sensor based context-aware service in ubiquitous home. In: Int. Conf. on Convergence Information Technology, Gyeongju, Republic of Korea, November 2007, pp. 1040–1047 (2007)

[14] Lee, H., Kim, J., Huh, J.: Context-aware based mobile service for ubiquitous home. In: 8th Int. Conf. Advanced Communication Technology, February 2006, vol. 3 (2006)

[15] Agarawala, A., Greenberg, S., Ho, G.: The context-aware pill bottle and medication monitor. In: Video Proceedings and Proceedings Supplement of the UBICOMP 2004 (2004)

[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] Jain, A.K., Bolle, R.M., Pankanti, S.: Biometrics: Personal Identification in a Networked Society. Kluwer, Norwell (1999).

[21] Daugman, J.: Biometric Decision Landscape,Technique Report No. TR482, University of Cambridge Computer Laboratory (1999)

[22] 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 implicitly in Fourth Amendment

[23] See. European Court of Human Rights, López Ostra v. Spain - 16798/90 [1994] ECHR 46 (9 December 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? In: Government Information Quarterly, vol. 16(2), pp. 87–91 (2001)

[24] Woodward, J.: Biometric scanning, law & policy: identifying the concerns-drafting the biometric blueprint. U. Pitt. L. Rev. 59, 97–155 (1998)

[25] Beck, U.: La sociedad del riesgo: hacia una nueva modernidad (1998)

[26] Jain, A.; Hong, L; Pankanti; S.: Biometric identification. In: Communications of the ACM, Vol. 43, No. 2, p. 91-98, (2000)

[27] Lin, Liou, Wu: Opportunities and challenges created by terrorism. Technological Forecasting and Social Change 74(2), 148–164, 158 (2007)

[28] Kennedy, G.: Thumbs up for biometric authentication. Computer Law Review & Tech. (8), 379–407 (2003-2004)

[29] Parejo Alfonso, Luciano: Seguridad pública y policía administrativa de seguridad, Valencia (2008)

[30] To see examples, http://www.biometrics.gov/Documents/FAQ.pdf (040809)

[31] 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, 23.11.1995, p. 31–50 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, 31.7.2002, p. 37–47. In the United States there is no general regulation on data protection. Kuner, C: An international legal framework for data protection: issues and prospects. Computer Law & Security Review 25, 307–317 (2009)

[32] Haas, Eric: Back to the future? The use of biometrics, its impact on airport security, and how this technology should be governed. In: Journal of Air Law and Commerce, No. 69, p. 459 y ss. (Spring 2004).

[33] Star, Greg: Airport security technology: is the use of biometric identification technology valid under the Fourth Amendment?: Law & Technology Journal No. 251, (2001-2002).

[34] Luther, Jörg: Razonabilidad y dignidad humana. In: Revista de derecho constitucional europeo, Nº. 7, ps. 295-326, (2007).

[35] Rodríguez de Santiago, J.Mª. La ponderación de bienes e intereses en el Derecho Administrativo. Madrid (2000).

[36] Kennedy. Note 28

[37] This type of regulatory systems has been used previously in access points in the frontiers of the European Union, where a specific regulation exists: 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 OJ L 385, 29.12.2004, p. 1–6 modified by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States OJ L 142, 6.6.2009, pp. 1–4

Authors

Juanita Pedraza is assistant professor of administrative law at the Universidad Carlos III de Madrid. Her research topics are telecommunications regulation, competition law, human rights and administrative law. She is researching her PhD thesis on UMT licenses in Spain, and she is a member of three research groups: Climate Change, Studies of Gender, and Information Society.

Miguel A. Patricio received his BSc in Computer Science in 1991, his MSc in Computer Science in 1995 and his PhD in Artificial Intelligence in 2002 all from the Universidad Politécnica de Madrid. He has held an administrative position at the Computer Science Department of the Universidad Politécnica de Madrid since 1993. He is currently Associate Professor at the Escuela Politécnica Superior of the Universidad Carlos III de Madrid and research fellow of the Applied Artificial Intelligence Group (GIAA). He has carried out a number of research projects and consulting activities in the areas of automatic visual inspection systems, texture recognition, neural networks and industrial applications.

Agustín de Asís is associate professor at the Universidad Carlos III de Madrid and research fellow of “Instituto Pascual Madoz”, center for research on urbanism. He received a PhD degree from the Universidad Complutense de Madrid in 1986 and has written many papers published in prestigious law reviews. He has carried out a number of research projects in the fields of urbanism, administrative law, telecommunications law and electronic commerce and is a member of “Estudio Jurídico” law firm integrated into Universidad Carlos III de Madrid.

José M. Molina is full professor at the Universidad Carlos III de Madrid. He joined the Computer Science Department of the Universidad Carlos III de Madrid in 1993. Currently he coordinates the Applied Artificial Intelligence Group (GIAA). His current research focuses on the application of soft computing techniques (NN, Evolutionary Computation, Fuzzy Logic and Multiagent Systems) to radar data processing, air traffic management, e-commerce and ambient intelligence. He has authored up to 20 journal papers and 80 conference papers. He received a degree in Telecommunications Engineering in 1993 and a PhD degree in 1997 both from the Universidad Politécnica de Madrid.