Regulatory Model for AAL

Juanita Pedraza, Miguel Angel Patricio, Agustin de Asís, and Jose Manuel Molina

Abstract. In this work, authors define a set of principles that should be contained in context-aware applications (including biometric sensors) to accomplish the legal aspect in Europe and USA. Paper presents 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.

Keywords: Context-Aware Applications, Ambient Intelligence, Privacy by Design, European Law, Human Rights.

1 Introduction

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 ambienece (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 [40]. AmI has also been recognized as a promising approach to tackle the problems in the domain of Assisted Living [41].

Ambient Assisted Living (AAL) born as an initiative from the European Union to emphasize the importance of addressing the needs of the ageing European

Juanita Pedraza · Agustin de Asís
University Carlos III de Madrid, Public Law Department, Avda. Univ. Carlos III, 22, 28270, Colmenarejo, Madrid, Spain
e-mail: {jpedraza,aeasis}@der-pu.uc3m.es

Miguel Angel Patricio · Jose Manuel Molina
University Carlos III de Madrid, Computer Science Department, Avda. Univ. Carlos III, 22, 28270, Colmenarejo, Madrid, Spain
e-mail: mpatrici@inf.uc3m.es, molina@ia.uc3m.es
population, which is growing every year as [42]. 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. [43], 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. [44] 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 [45] 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 [46] 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. Before the inclusion of biometric sensors, identity and location were the main problems of privacy in context applications. Works in the literature have addressed these privacy problems from two different views, the first one centered in the development of frameworks [9] [10] and the second one centered in searching some degree of user anonymity [12] [13] [14].

In [14], these two ideas are combined in a framework with anonymity levels. Authors focus on the privacy aspects of using location information in pervasive computing applications. The tracking of user location generates a high amount of sensitive information. Authors consider privacy of location information as controlling access to this information. The approach is a privacy-protecting framework based on frequently changing pseudonyms, so users avoid being identified by the locations they visit. Agre [8] has advocated an institutional approach that casts privacy as an issue not simply of individual needs and specific technologies, but one that arises from recurrent patterns of social roles and relationships.

The inclusion of 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 threat to privacy [15]. European and American judges [16] have categorized privacy as taking three distinct forms. These includes [17]: 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.