Chapter 12

Privacy in Pervasive Systems:
Legal Framework and
Regulatory Challenges

Antonio Liotta
Technische Universiteit Eindhoven, The Netherlands

Alessandro Liotta
Axiom - London, UK

ABSTRACT

Data protection legislation has developed in a digital communication context that is changing dramatically. Infrastructure-based, networked systems are increasingly interconnecting and interoperating with infrastructure-less or even spontaneous networks, which are important elements of pervasive systems. These are also characterized by an autonomic, self-managed behavior that undermines the role of central management entities such as network and service providers. In this context, meeting the demanding requirements of privacy laws becomes a serious challenge, because once the user’s data crosses a managed boundary, it is impossible to clearly determine and transfer responsibilities. This chapter revisits the important elements of privacy regulations with the purpose of highlighting the hurdles posed onto pervasive systems. The analysis in this chapter identifies imperative research and technological issues.

INTRODUCTION

The treatment of personal information has become a sensitive topic for businesses, governmental authorities and individuals. During the past years, the number of data security breaches occurred has significantly increased, raising great concern in the public opinion. Consumers expect that appropriate technical measures are in place at all times to avoid unauthorized access to their personal data.

The new century is seeing deep technology improvements in the communications arena. This represents, at the same time, a great opportunity for the users, who are now able to benefit from a
wider variety of services available via different devices, but also a greater threat to their privacy.

Data protection regulations have been in place for several years in almost all countries around the world, but their effectiveness is now being questioned by individuals and businesses in the light of the potential impact that new technologies may have on the individuals’ private life.

To this respect, pervasive computing is expected to represent a new challenge for the society (Hansmann, 2003). The intrusiveness of such new communications technology together with the lack of control that (unlike the more traditional networked systems) characterizes its networks, if not addressed adequately, may result in a loss of individuals’ trust in pervasive technology. The need to gain customers’ confidence and the obligation to comply with all applicable regulations will then impose a great pressure on businesses willing to invest in such technology.

In this chapter, we give an overview of the privacy legislation and its potential impact on the commercial development of pervasive computing, through the analysis of court cases in Europe. We also give a first cut consideration of the potential conflicts between privacy regulations, data retention obligations and copyright infringement protection that may arise in a global environment from the application of pervasive systems, and how these issues are to be seen as topics to put to the attention of businesses, researchers and regulators.

Our review unveils key shortcomings of the current legal framework specifically in relation to pervasive systems. Data protection legislation has developed in a digital communication context that is changing dramatically. Particularly, the role and responsibilities of data controllers, network operators, and service providers are blurred in a pervasive system where networks span across different domains, organizations and countries. Also, several portions of the network tend to be self-managed rather than being under the direct control (and responsibility) of a named entity.

By contrast to a more conventional (non-pervasive) networked system, where it is relatively easier to determine who is responsible for privacy compliance and can transfer those responsibilities among data processors, in pervasive systems this is not always possible. The very idea of pervasiveness is associated with the concepts of “ubiquity”, “transparency”, “distribution”, and “autonomic management”. Pervasive networks include not only infrastructure-based technologies (such as WiFi, cellular systems, ADSL), which rely on management entities that can be held responsible for the data flow. Pervasive networks are increasingly made of infrastructure-less (or spontaneous) network elements (such as ad hoc networks, MANETs, or sensor networks) (Sarkar, 2007), in which cases the user’s terminal has the potential to transparently store or relay data belonging to other users.

Hence, the very nature of a pervasive system clashes head-on with the very essence of privacy regulatory principles. In order to fully appreciate the controversial legal issues surrounding pervasive systems, this chapter focuses on the current data protection legal framework.

The following section provides the necessary background, introducing key data protection concepts and definitions. We then present the eight fundamental principles underlying the Data Protection Directive. These are further illustrated with the aid of four case studies. Having introduced the relevant legal framework, we finally place it in the context of pervasive systems, which helps understanding the hurdles and risks of pervasive systems (in their current form and their future development), giving an indication of the most crucial technological and research issues.
Related Content

The Design of Portable Integration Strengthening Machine
www.igi-global.com/chapter/design-portable-integration-strengthening-machine/72936?camid=4v1a

Ambient Intelligence on the Dance Floor
www.igi-global.com/chapter/ambient-intelligence-dance-floor/37876?camid=4v1a

Inventory Control and Replenishment of Multi-Product Multi-Echelon Based on Time Cost Under JMI Environment

An Adaptable Context Management Framework for Pervasive Computing
www.igi-global.com/chapter/adaptable-context-management-framework-pervasive/37793?camid=4v1a