Chapter 7.9
Privacy Control Requirements for Context-Aware Mobile Services

Amr Ali Eldin
Accenture BV, The Netherlands

Zoran Stojanovic
IBM Nederland BV, The Netherlands

ABSTRACT

With the rapid developments of mobile telecommunications technology over the last two decades, a new computing paradigm known as 'anywhere and anytime' or 'ubiquitous' computing has evolved. Consequently, attention has been given not only to extending current Web services and mobile service models and architectures, but increasingly also to make these services context-aware. Privacy represents one of the hot topics that has questioned the success of these services. In this chapter, we discuss the different requirements of privacy control in context-aware services architectures. Further, we present the different functionalities needed to facilitate this control. The main objective of this control is to help end users make consent decisions regarding their private information collection under conditions of uncertainty. The proposed functionalities have been prototyped and integrated in a UMTS location-based mobile services testbed platform on a university campus. Users have experienced the services in real time. A survey of users' responses on the privacy functionality has been carried out and analyzed as well. Users' collected response on the privacy functionality was positive in most cases. Additionally, results obtained reflected the feasibility and usability of this approach.

INTRODUCTION

Despite the expected benefits behind ambient technology and the need for developing more and more context-aware applications, we enunciate that privacy represents a major challenge for the success and widespread adoption of these services. This is due to the collection of a huge amount of users' contextual information, threatening their

privacy concerns. Controlling users' information collection represents a logical way to let users get more acquainted with these context-aware services. Additionally, this control requires users to be able to make what is known as *consent* decisions, which face a high degree of uncertainty due to the nature of this environment and the lack of experience from the user side with information collectors' privacy policies. Therefore, intelligent techniques are required in order to deal with this uncertainty.

Context-aware applications are applications that collect user context and give content that is adapted to it. There have been different scenarios in the literature that describe how a context-aware application would look. Mainly, the idea is that the user's environment is populated with large numbers of sensors that collect information about users in order to provide useful content or services that are adapted to his or her context. Although this personalized functionality would be very helpful for the user, it allows collecting parties to know sensitive information about users that can violate their privacy, unless these applications have taken special measures and practices to support their privacy needs.

Informed consent is one of the requirements of the European Directive (2002). Accordingly, a user should be asked to give his or her informed consent before any context collection. From a usability point of view, it will be difficult to let each user enter his or her response each time context is collected. Increasingly, the type of collected data will highly influence his or her privacy concerns. The problem becomes even more complex when more than one party gets involved in collecting user information, for example third parties. Third parties of a certain information collector represent unknown parties to the user. Despite that the first information collector might list in its privacy policy that user information is being given to those third parties in one way or another, it is not possible yet in the literature (Hauser & Kabatnik, 2001) to provide a means for the user to know which party collects which information. Thus uncertainty takes over when a user gets pushed information or services from unknown collectors whether to give them consent or not.

PROBLEM DESCRIPTION AND RELATED WORK

In this section, we discuss the motivation behind this work and the type of research problem we are addressing. The problem investigated in this work can be seen as a multidisciplinary problem where legal, social, and technical domains are concerned with providing solutions. In this work, we focus on the technological perspective, taking into consideration requirements set by the other domains.

There is a trade-off between users' privacy needs and their motivation behind giving private information away. Complete privacy is impossible in a society where a user would have to interact with other members of the society such as colleagues, friends, or family members. Each flow of user information would reveal some private information about him or her, at least to the other destination. Since this flow of information is needed and may be initiated by the user, he or she would have to make sure that the other party (the destination) is going to keep his or her privacy requirements. Privacy policies and legal contracts help users and service providers reach an agreement on the type of privacy users would have. However, these contracts do not provide enough flexibility for users on choosing the type of privacy they need. It also does not guarantee that their privacy will not be violated, but it guarantees that the user would have the rights to sew them if these agreed-upon contracts were violated.

Privacy-enhancing technologies (PETs) are assumed to help reduce privacy threats. Privacy threats emerge as a result of the linkage between identities and users' contextual data. Therefore, most literature has focused on the separation