Chapter 3.6
Dynamic Control Mechanisms for User Privacy Enhancement

Amr Ali Eldin
Accenture, The Netherlands

ABSTRACT

Despite the expected benefits behind context-awareness 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 huge amount of users' contextual information, which would highly threaten 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 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. In this chapter, the auhtors propose a consent decision-making mechanism, ShEM, which allows users to exert automatic and manual control over their private information. An enhanced fuzzy logic approach was developed for the automatic decision making process. The proposed mechanism has been prototyped and integrated in a UMTS location-based services testbed 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' response on the privacy functionality was positive. Additionally, results obtained showed that a combination of both manual and automatic privacy control modes in one approach is more likely to be accepted than only a complete automatic or a complete manual privacy control.

DOI: 10.4018/978-1-61350-323-2.ch3.6

INTRODUCTION

Advances in mobile network access technology with increasingly higher bandwidth capacity, intelligent mobile devices, and smart miniaturized sensors, have opened up a whole range of new possibilities. Ubiquitous computing brings new challenges to information and computer science; one of those challenges is to deal with privacy threats, how to present sensitive information about individuals such as location, preferences and activities. In addition, the possibility that users' profiles may be shared among different parties without the user's consent may also pose a serious threat to user privacy. For example, mobile health applications make it possible to monitor patients who might become ill due to a disease: for instance to prevent epileptic seizures or hypoglycaemic conditions in case of diabetics, especially during times when their treatment is being set-up or adjusted. Small medical sensors combined with higher bandwidth and more reliable mobile network technologies make it possible for such patients to be monitored and even treated anytime and anywhere. This allows patients to live more 'normal' lives, and it helps improve their quality of life and well-being. However, it also has a serious impact on a patient's privacy, a factor that should be given serious consideration.

There is a trade off between a user's privacy requirements and the reasons he or she may have to allow information to be made available. Complete privacy is impossible in a society where a user has to interact with other members of the society such as colleagues, friends, or family members. Each flow of user information will reveal some private information about the user at least to the information receiver. Since this flow of information is needed, and maybe self-initiated by the user, a user needs to make sure that the other party (the destination) is going to adhere to his or her privacy requirements.

Privacy policies and legal contracts can be used to help users and service providers reach an agreement on the type of privacy users will have. However, these contracts do not provide enough flexibility for users with respect to choosing the type of privacy they need. They also do not guarantee that a user's privacy will not be violated but what they do is that they give the user the right to sue an organization if the privacy contract was broken. Although a lot of efforts on privacy protection has been exerted in the literature (Ackerman, Darrell, & Weitzner, 2001; Camenisch & Herreweghen, 2002; Casal, 2001), not many efforts has realized the option that privacy could be negotiable. A user Ben might be willing to share his information with information collectors in order to get some cheaper service or a better offer. What makes it complex is that users' privacy concerns could be influenced not only by mostly known factors such as culture, age, etc., but also by their context or situation when the information is requested. This influence of context becomes noticeable in environments where users context is expected to change.

Context may be defined as any information that can be used to characterize the situation of an entity, where an entity can be a person, place, physical or computational object that is considered relevant to the interaction between an entity and an application. Contextual information matches any relevant object in the user's environment or user description: examples would be Ben's location, time, mobile device capabilities, network bandwidth, etc. Contextual information can come from different network locations, protocol layers and device entities. Context-aware applications are applications that collect users' context and give content that is adapted to it.

Informed consent is one of the requirements of privacy set up by the European directives (EuropeanDirective, 2002). Accordingly, a user should be asked to give his/her informed consent before any context collection. From a usability point of view, it would be difficult to let each user enter his/her response each time context is collected. Increasingly, the type of collected data would