IGI PUBLISHING **ITJ3909**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, International Journal of Information Security and Privacy, Volume 1, Issue 4
edited by **Hamid R. Nemati © 2007, IGI Global**

Towards Autonomous User Privacy Control

Amr Ali Eldin, Delft University of Technology, The Netherlands

René Wagenaar, Delft University of Technology, The Netherlands

ABSTRACT

In this article, we 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 are more likely to be accepted than only a complete automatic or a complete manual privacy control.

Keywords: *context awareness; fuzzy logic; fuzzy systems; mobile technologies; privacy control, user preferences description, user prototypes*

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 and 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 the user 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 may be self-initiated by the user, a user needs to make sure that the other party (the destination) is going to adhere to the 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 give the user the right to sue an organization if the privacy contract was broken. Although a lot of efforts on privacy protection have been exerted in the literature (Ackerman, Darrell, & Weitzner, 2001; Camenisch & Herreweghen, 2002; Casal, 2001), not many efforts have 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, and so forth, 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, and so forth. 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 informed consent before any context collection. From a usability point of view, it would be difficult to let each user enter a response each time the context is collected. Increasingly, the type of collected data would highly influence the user's privacy concerns. The problem becomes more complex when more than one party gets involved in collecting users 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 users 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 Ben gets pushed information or services from unknown collectors whether to give them access or not. Although he did not give explicit consent to unrelated third parties in his privacy preferences, he did not mention he would block them either.

Privacy strictness varies from one user to another. It is not possible to generalize it or to have a common agreement on which data elements should be given away and which should not since privacy is mainly a personal matter. In this sense, Ben should be able to define how he thinks his personal information should be dealt with, which information practices are acceptable, and which ones he does not approve in what is known as privacy preferences description. Although this might look simple, defining effective preferences that match each user and that is efficient in describing their privacy needs is still immature (Ali Eldin & Wagenaar, 2004). When a lot of application domains get involved in exchanging Ben's information with different types of information demands and different types of services,