Context Data Model for Privacy

Emin İslam Tatlı
Department of Computer Science, University of Mannheim, Germany
tatli@informatik.uni-mannheim.de

PRIME Standardization Workshop
IBM Zürich, 06-07 July 2006

Abstract

Context-aware applications introduce new privacy risks while utilizing user context data. Location is the most benefited context that is taken into consideration within context-aware applications. But there are more context than location and more privacy risks than location privacy risks. In addition, there is a context to context relation in terms of privacy. In this paper, we propose a privacy-aware context data model based on the context data model of Schmidt et al. The proposed data model focuses on context privacy and privacy dependence of context-to-context relations.

1 Motivation

Context-aware applications use context as input when delivering a service. Context-aware applications can be grouped into different six groups [2]: tracking services, navigation services, information services, communication services, entertainment services and transaction services. Context can be described as any information that can be used to characterize the situation of an entity, like a user's identity, habits, emotions, etc. Location is the most dominant context used within applications.

In location-aware applications, users' absolute or relative location is used as input to the system and the service is returned accordingly. Geographical positioning system (GPS) is the common method to compute the location in outdoor. Wlan and bluetooth access points-based techniques are used to calculate the location in indoor areas. Even though location enables very useful functionality, collecting location data and tracking people have become the new privacy risks in location-aware applications. Considering the risks, the users should be in the position to control their location privacy.

Even though location is the most used context, there are other context data that increase functionality. Schmidt et al. point out this fact within their paper titled *"There is more to Context than Location"* [6] and propose a *context data model* which illustrate possible context data stemming from the user himself and his surroundings.

Supporting more context data means dealing with more privacy risks about the new context data. Besides, each context data can affect the privacy level of other context data and this makes the privacy control more difficult. Future context-aware applications should take into consideration the context privacy of users and the dependence of context relations. Hence, a new context data model is required to integrate within future applications. In this paper, we have reworked the context model proposed by Schmidt et al. and enhanced it to a new data model with privacy concerns in mind.

The paper is structured as follows: In Section 2, the context data model of Schmidt et al. is explained. Privacy requirements of context data in the new data model are discussed in Section 3. The proposed privacy-aware data model is explained in Section 4. Finally, the paper is concluded.

2 Context Data Model

Schmidt et al. go beyond location and introduce more context data about a user and his environment. Their proposed data model is illustrated in Figure 1.

According to the their model, context can originate from *human factors* or *physical environment*. Human factors can be categorized into three as user (his knowledge, characteristics, habits, etc.), social environment (social interaction, etc.) and tasks (engaged tasks, general goals, etc.). Physical environment can be also categorized into three as conditions (light, audio, temperature, etc.), infrastructure (surroundings for computation and communication) and location (absolute location, relative location, etc.).

The main focus of this data model is the context resources. It does not consider context privacy and context interactions.

3 Privacy Requirements

Existing works [1, 3, 4, 5] on context privacy consider a small set of context like location, date and time. But new context-aware applications will use

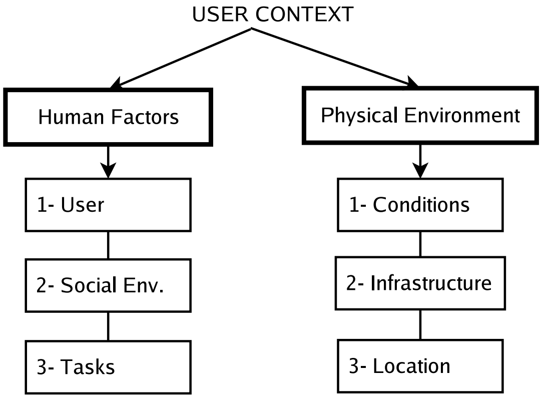

Figure 1: User Context Data Model

more context data and therefore a new *privacy-aware* data model is needed. In this new model, the following privacy issues should be defined in details:

a) Context data should be classified as *protected* and *not protected.* Not all context data are shared with others within the applications. The context-data that are distributed to others should be *explicitly* defined within *protected* context group.

b) Status of a context data can change very often and this change can affect the user's privacy preferences over his another context. For example, the change in the social environment can affect your privacy concern on location context. You may want to hide your location from others except your family members.

c) Context *blurring* enables a user to give away the value of his context within ranges, instead of giving the exact value. It can be used as a method to increase privacy. The context data that can be blurred should be explicitly defined in the new data model.

4 Privacy-aware Context Data Model

Analyzing Schmidt et al.'s context data model and the privacy requirements in the previous section, we have come up with two main categories in the privacy-aware context data model. *protected context* and *evaluated context.*

The context data in the protected context group are distributed to other principals in order to increase the functionality and therefore require privacy

A. Protected Context	*Content*
1. User Identity	personal data like name, address, phone number, birth date, credit card number, etc.
2. User Profile	user interests, characteristics, habits, schedule, etc.
3. Physical Conditions	the context around the physical surroundings like temperature, light, pressure, etc.
4. Location	the absolute or relative location of a user
B. Evaluated Context	*Content*
5. User Morale	user's psychological morale status
6. Infrastructure	the surrounding resources with communication capability
7. Social Environment	user's relatives, neighbors, colleagues and their relationships
8. User Tasks	the user's assigned tasks and aims
9. Time	date, time and day of week

Table 1: Privacy-aware Context Data Model

protection. Any context data in this group can get benefit of blurring. The context data in the evaluated context group are not sent to other principals, but affect user's privacy concerns and therefore are used to evaluate the privacy of the context data in the protected group. Table 1 explains the context data of each group in details:

Privacy dependence of context data and blurring functionality in our privacy-aware model are illustrated in Figure 2. In our model supporting context privacy dependence, the main focus is on the *protected* context. The user's exchanged context should be protected and for this purpose privacy policies based on context data from both protected and evaluated context group can be used. As an example of *protected2protected* context privacy dependence; a user can reveal his location (*context to protect*) to only people who is at a certain location (*context as protector*) or who has a certain identity (*context as a protector*). As an example of *protected2evaluated* context dependence; you may not reveal your identity or location (*context to protect*) at certain dates *(context as protector)*, e.g. during holiday.

User task is concerned with the tasks and aims of a user and belongs to the evaluated context data group. User morale (i.e. angry, sad, happy, etc.) also belongs the evaluated context data group. But they can not be used

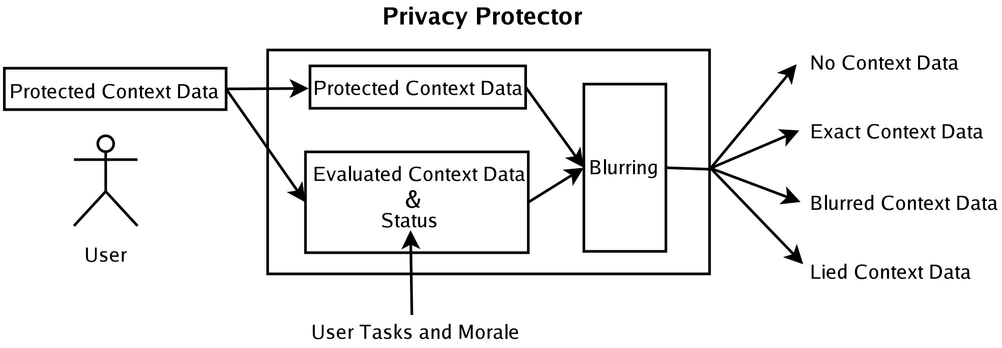

Figure 2: Context Interaction in Privacy-aware Data Model

directly for context evaluation. But having many tasks, being busy or sad for a particular period, the user can change his status which then can be used as a privacy protector to evaluate.

Additionally, context blurring policies can also be defined based on both protected and evaluated context privacy. As examples, the user can blur his location if his status is set to *away* or the user can blur his characteristics information according to the physical conditions.

5 Conclusion

In this paper, we have proposed a privacy-aware context data model which can help the management of privacy in context-aware applications. The proposed data model defines a set of context data as the protected context group and supports defining privacy policies on the protected group based on any context data originated from the user himself or his surroundings.

References

[1] Platform for Privacy Preferences(P3P) Project. http://www.w3c.org/P3P. World Wide Web Consortium.

[2] H. H. Bauer, T. Reichardt, and A. Schüle. Was will der mobile Nutzer? Forschungsergebnisse zu den Anforderungen von Nutzern an kontextsensitive Dienste. University of Mannheim, 2006.

[3] Ginger Myles et al. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 2(1):56–64, 2003.

[4] M. Zuidweg et al. Using p3p in a web services-based context-aware application platform. http://www.w3.org/2003/p3p-ws/pp/utwente.pdf.

[5] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *UbiComp '02: Proceedings of the 4th international conference on Ubiquitous Computing*, London, UK, 2002.

[6] Albrecht Schmidt, Michael Beigl, and Hans-W. Gellersen. There is more to context than location. *Computers and Graphics*, 23(6):893–901, 1999.