

# PRIVACY IN CONTEXT-AWARE MOBILE BUSINESS APPLICATIONS

Emin Islam Tatli

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

## ABSTRACT

Privacy is a big barrier for the acceptance of mobile business applications. Users require full privacy control over their context data like identity, time schedule, profiles, location, etc. Platform for Privacy Preferences (P3P) from W3C proposes a privacy solution for internet users. The aim of this PhD is to extend P3P to support user-centric privacy aspects in both pull and push services regarding context-aware mobile business applications. As a preliminary work, a privacy context data model from the privacy perspective will be formally described. Afterwards, P3P extension for the privacy architecture and policies will be designed. The required security protocols and cryptographic methods will be developed to enforce privacy with P3P policies. The proposed P3P extension will be integrated within the applications of an existing mobile business framework.

## KEYWORDS

User-centric privacy, context-aware mobile business

## 1. CONTEXT-AWARE APPLICATION

The m-business research group [4] at the University of Mannheim aims at developing a generic framework for context-aware mobile business applications. Context-aware mobile business applications consider context of mobile users as input when delivering their services. There are six different types of context-aware applications according to Bauer et al. [8]: Person or object *tracking* services, *navigation* services, *information* services, *communication* services, *entertainment* services and *transactional* m-commerce services.

Context-aware services can be also grouped as pull and push services. In pull services, the user gets the service upon his request. Navigation, information and transaction services belong to pull services group. In push services, the user joins a service, sends regularly some of his context data like location to a central server and other principals can use the user's context data to push a service to the user. Tracking, communication and entertainment services belong to push services group.

A mobile user can be interested in using many different pull and push context-aware service via his mobile device and share his context with other persons or service providers for the sake of functionality. But privacy of their context becomes the doubts of the users which can prevent them using the services. The users can be afraid of the fact that their location is collected and they are tracked, or their context data is together evaluated to reveal the real identity of the user, etc. Besides, the EU commission has published two directives [3,2] in 1995 and 2002 for the legacy aspects of respecting personal data privacy. Hence, context privacy should be satisfied and users should be in the position to control their context privacy.

## 2. REVIEW OF PRIVACY LITERATURE

P3P (*Platform for Privacy Preferences*) [5] is a project of W3C and aims to protect internet users against the web privacy risks. In P3P, web servers publish their privacy policies which explain in details what type of

data they collect and why, whether they can personally identify people from the collected data and who can see this data. User privacy agents retrieve the server privacy policies, compare with the user preferences expressed in Appel (a P3P Preference Exchange Language) [1] and decide whether or not to access to the server. P3P is designed for web platform and does not support context-aware applications. As a further development of P3P, Wasp project aims to extend P3P for context-aware applications. But their scope for the context is limited to location and date as context properties [11, 9, 18]. Dynamic context properties like *status* (as its importance implied in [14]), the privacy relations between different context data are not taken into consideration. Besides, no real integration and user usability tests were done in Wasp.

There are other research works that consider privacy for dynamic and ad-hoc environments, but not specifically for user-centric privacy in context-aware applications. Myles et al. [10] designed an architecture based on P3P for preserving privacy in location-based applications. Users send their privacy preferences when registering to the location server; applications send their privacy policies and server-side validators compare the user preferences and the application policies.

In paws [13], a user enters in an area where different sensor devices collect user data. The user agent retrieves the devices' policies and compares them with the user preferences.

E-P3P (Enterprise Privacy Practices) [6] was IBM's first attempt to propose a privacy model to support privacy requirements and enforce policies within enterprises. EPAL (The Enterprise Privacy Authorization Language) [7], as a successor of E-P3P, was designed by IBM and submitted to W3C to become a standard. Unlike P3P, EPAL takes into consideration of enforcement of privacy rules. But unlike our user-centric concerns, EPAL focuses on B2B privacy domain.

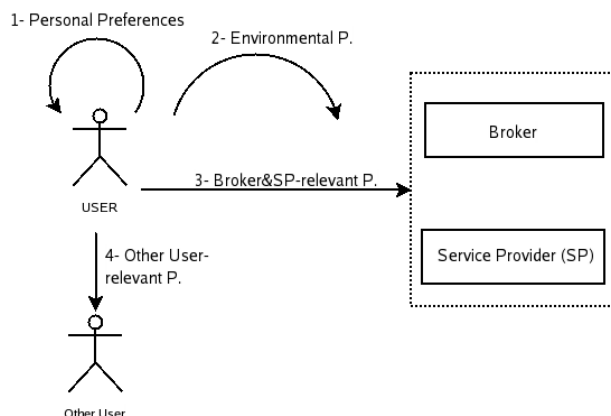
The identity manager tool [12] helps users to control of their transmitted data to certain applications in e-commerce applications. But the need to assign a privacy preference for each individual application decreases usability as emphasized in [14].

### 3. NEW REQUIREMENTS FOR CONTEXT PRIVACY

Examining the architecture of context-aware systems, we have realized that the privacy concerns should not be considered only from one principal's perspective and/or one specific data type like location. For example, P3P considers the user privacy aspects only from the service provider side. But for enabling a more complete privacy solution, all user privacy aspects as illustrated in Figure 1 should be taken into consideration. A user's privacy concerns can be stemmed from *his personal preferences* like identity, status (i.e. busy, away, etc.), *the environment* like indoor/outdoor application, *the broker/service providers* and *other users*.

Existing works [11] about context privacy consider only a few context data like location and date. But there is more context beyond location. Schmidt et al. point out this fact within their paper titled "*There is more to Context than Location*" [15] and propose a *context data model* which show possible context data stemming from the user himself and his surroundings.

Figure 1. Privacy Concerns of Users



Besides, there is a context-to-context relation for the privacy sensitivity of a user over his context and we have not come across with any work considering these relations. For example, a user may reveal his location to persons who hold a certain property like being within a certain place. Considering this relation, based on Schmidt et al.'s context data model, we have proposed a privacy-aware context data model [16] which groups context data as *protected context* and *evaluated context* as shown in Table 1. The context data in the *protected context* group is shared with others therefore requires privacy protection. On the other hand, the context data in the *evaluated context* group is not transmitted to others, but affects the privacy level of the context data in the protected group. In Table 1, each subgroup is explained with examples.

This context model would help to specify privacy policies based on context-to-context dependence. Within a further paper [17], we explained context-to-context dependence within privacy policies based on the privacy-aware context model. As an example of *protected2protected* context privacy dependence; a user can reveal his location (*context to protect*) to only people who are 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 want to reveal your identity or location (*context to protect*) at certain dates (*context as protector*), e.g. during holiday.

Table 1. Privacy-aware Context Data Model

<b>Protected Context</b>	<i>Content</i>
1. User Identity	personal data like name, address, phone number, birth date, credit card number, etc.
2. User Profile	user interests, characteristics, habits, time 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</b>	<i>Content</i>
5. User Morale	user's psychological morale status
6. Infrastructure	the surrounding resources with communication capability
7. Social Environment	user's relatives, friends, other users, service providers and their relationships
8. User Status	the user's busyness due to his assigned tasks and aims
9. Time	date, time and day of week

#### 4. FUTURE WORK

Our main goal is to design user-centric privacy architecture by extending P3P for context-aware applications. Within a six-month period, we have proposed a privacy-aware context data model which shows different context data of mobile users from the privacy perspective and the context-to-context relations. In addition, privacy policies explaining context-to-context relations based on the privacy-aware data model were explained within another paper. As a future work, we are planning to focus on the following topics:

1. *Formal specification of the context model*: The proposed privacy-aware data model is currently more at an abstract informal level. The context data in each context subgroup of the privacy aware data model needs to be formally specified in a concrete way. Providing this, these context data can be integrated within the P3P extension.

2. *Designing privacy architecture and extending P3P*: P3P will be examined to be extended for supporting the privacy-aware data model and thus context-aware applications (both for pull and push services). Based on the P3P extension, user-centric privacy architecture will be designed.
3. *Policy enforcement*: The relevant cryptographic methods and security protocols that are required to enforce privacy policies will be implemented.
4. *Privacy policy specification and integration*: The extended P3P policies will be used to specify privacy policies and integrated within the pull and push applications from the m-business framework.
5. *Usability experiments*: Usability tests need to be done with the end users. When extending the P3P, usability of the privacy policies would be the main challenge, because there is a trade-off between security and usability. The systems that are not user-friendly designed are not well accepted by users and their security mechanisms fail.

## 5. CONCLUSION

Designing a user-centric privacy architecture based on extending P3P for context-aware mobile business applications is the main focus of this PhD work. To guarantee full control over privacy, a user's all privacy concerns regarding the user himself, the environment, the broker and service providers and other users should be taken into consideration. The standard privacy solution P3P from W3C takes only user-service provider relations into consideration. We would extend P3P to support context aware applications. As a preliminary work, we have proposed a privacy-aware context data model that explicitly defines the context data to be protected and the context data to be evaluated during the policy enforcement. Privacy policies with the focus context-to-context relations based on the proposed data model was explained further within another paper. Formal definition of the privacy-aware context data model, extending P3P by integrating the privacy-aware context data model within, integrating the extended P3P privacy policies within the m-business applications and doing experimental usability tests compose the future focus of this PhD.

## ACKNOWLEDGEMENT

The work described in this paper has been supported by the "Landesstiftung Baden-Württemberg" and the Ministry of Science, Research and Arts of the state of Baden-Württemberg.

## REFERENCES

- [1] A P3P Preference Exchange Language (Appel). <http://www.w3.org/TR/P3P-preferences/>.
- [2] EU Directives 2002/58/EC. [http://www.dataprotection.ie/documents/legal/directive2002\\_58.pdf](http://www.dataprotection.ie/documents/legal/directive2002_58.pdf).
- [3] EU Directives 95/46/EC. <http://www.cdt.org/privacy/eudirective/EU Directive .html>.
- [4] The mobile business research group. <http://www.m-business.uni-mannheim.de>.
- [5] Platform for Privacy Preferences (P3P) Project. <http://www.w3c.org/P3P>. World WideWeb Consortium.
- [6] P. Ashley, S. Hada, G. Karjoth, and M. Schunter. E-p3p privacy policies and privacy authorization. In *Proc. of the ACM workshop on Privacy in the Electronic Society (WPES 2002)*, pages 103–109. ACM Press, 2002.
- [7] P. Ashley, S. Hada, C. Powers, and M. Schunter. Enterprise privacy authorization language (EPAL). Technical Report 3485, IBM Research, 2003.
- [8] H. H. Bauer, T. Reichardt, and A. Schüle. Was will der mobile Nutzer? Forschungsergebnisse zu den Anforderungen von Nutzern an context sensitive Dienste. University of Mannheim, 2006.
- [9] Chiel Drost. Privacy in context-aware systems. Master's thesis, University of Twente, 2004.
- [10] Ginger Myles et al. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 2(1):56–64, 2003.
- [11] 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>.

- [12] Uwe Jendricke and Daniela Gerd tom Markotten. Usability meets security -the identity-manager as your personal security assistant for the internet. In *Proceedings of the 16th Annual Computer Security Applications Conference*, pages 344–353, December 2000.
- [13] 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.
- [14] Scott Lederer, I. Hong, K. Dey, and A. Landay. Personal privacy through understanding and action: five pitfalls for designers. *Personal Ubiquitous Comput.*, 8(6):440–454, 2004.
- [15] Albrecht Schmidt, Michael Beigl, and Hans-W. Gellersen. There is more to context than location. *Computers and Graphics*, 23(6):893–901, 1999.
- [16] Emin Islam Tatlı. Context data model for privacy. In PRIME Project Standardization Workshop, Zürich, 2006. IBM.
- [17] Emin Islam Tatlı and Dirk Stegemann. Context privacy with context evaluation, paper submitted.
- [18] Martjin Zuidweg. A p3p-based privacy architecture for a context-aware services platform. Master's thesis, University of Twente, 2003.