To Share or not to Share: Supporting the User Decision in Mobile Social Software Applications

Giuseppe Lugano, Pertti Saariluoma
Social ICT – Human Dimensions Research Group,
University of Jyväskylä, Finland
gilugano@cc.jyu.fi, psa@it.jyu.fi

Abstract. User's privacy concerns represent one of the most serious obstacles to the wide adoption of mobile social software applications. In this paper, we introduce a conceptual model which tackles the problem from the perspective of trade-off between privacy and trust, where the user takes the decision with minimal privacy loss. To support the user decision, we introduce the Mobile Access Control List (Macl), a privacy management mechanism which takes into account the user attitude towards mobile sharing, his communication history and social network relationships.

Keywords: Privacy, Sharing, Trust, Mobile Social Software.

1 Introduction

Today, more than two billion people daily use mobile phones to communicate, mostly calling or sending text messages. The shift from second to third generation (3G) has transformed mobile phones into mobile multimedia computers, which are able to connect to the Internet, take pictures, record clips or watch movies, just to mention some of the features not available a few years ago. Although they are not yet widely spread, mobile data services are expected to grow in the coming years, while voice call revenues decrease. In particular, successful social web paradigms, like blogs and media sharing Internet services, will be accessible and integrated with mobile devices through mobile social software applications (MoSoSo), typically running on Smartphones and PDAs. Extending Shirky's definition of social software MoSoSo has been previously defined as a *kind of software that supports interaction among networked mobile users* [10]. Thus, it is a class of mobile applications whose scope is to support social interaction among interconnected users, with the emphasis of collaboration and data sharing. In some cases, MoSoSo is implemented by the vendor, as in the case of Nokia [13] or developed by third parties [6]. Being personalization through contextual data one of the salient characteristics of MoSoSo, one of the most serious obstacles to their adoption is represented by users' privacy concerns. Hence, there is need of providing effective mechanisms for privacy management of personal data.

2 Theoretical Background

2.1 Mobile Privacy Management

Social interaction is a complex phenomenon; although a lot of research and theories have been proposed, there is not a single framework to explain human social behavior. A classic framework, very influential in HCI, although originally developed for face-to-face settings, has been introduced by Erving Goffman [8]. More recently, researchers have studied how individuals perceive their status in social groups [2]. Human social behavior has been studied also from other perspectives; for example, marketing literature suggests that it is motivated mainly by value, which is shaped by both economic (utility related) and psychological (needs related) factors [3]. Benefits can be either extrinsic or intrinsic [5].

Theories of human social behavior have been utilized in mobile and ubiquitous computing environments to investigate privacy concerns [1,4,9,16] and they typically take into account not only individual needs, but also recurrent patterns of social roles and relationships. An important aspect of the problem concerns the identification of the parameters to consider when designing for privacy in the mobile context. One of them is certainly privacy harm, defined also as user's global privacy sensitivity [14]. This parameter has been studied as an individual utility maximization problem from the user - service provider perspective, making a distinction between general and individualized privacy policies. When considering the trade of personal data between end users, such policies do not exist and are often agreed time by time. As Raento observes [15], "*the privacy of a piece of data is approximately equal to the expected benefit you can gain from disclosing it, minus the expected harm that may come from disclosing it*". Analyzing the problem from the perspective of the trade-off between privacy and trust [17], the user choice follows a process which consists of the following steps:

1 Decide whether to trade trust for privacy or not
2 Determine minimal privacy damage
3 Compute trust gain
4 Trade privacy for trust if trust gain is greater than minimal privacy damage
5 Selection: user selects the set with minimal privacy loss

3 Mobile Privacy Management Design

3.1 General Approach

Observing the model suggested in [17], there are two core elements needed to let the user make a selection: the computation of trust gain and estimation of minimal privacy damage. Here, we assess such attributes on the basis of three dimensions: the

user, the recipient and the data. From the system perspective, users are represented by their profile, containing not only data which is visible to others (name, phone number, date of birth, photo…), but also an hidden section, which consists of mobile usage patterns, attitudes towards sharing and history of social behavior, expressed by communication logs of past interaction with his social network. Communication history and system usage patterns can support the user in a number of ways; for instance, to automatically infer and measure his social network [7]. Here, user's communication logs, together with information present in the user profile, are used to assess the level of acquaintance with a certain contact. With appropriate algorithms, such as the ones suggested in [11], it is possible, making some simplifications, to translate the data logs, which represent the network distance, into social distance. This process has its roots in Moreno's sociometric measurement [12], which has been very influential in the field of Social Network Analysis.

3.2 Minimal Privacy Damage

Although one of the steps of the privacy-trust trade-off problem is the computation of privacy damage, we consider here the privacy sensitivity perceived by the user for any kind of information that can be shared. Obviously, there is a relation between the two parameters: for low sensitivity items, the potential privacy damage is small. On the contrary, for very sensitive items, the value of privacy damage is high.

The easiest way to assess the privacy sensitivity associated with sharable items is to ask the user his opinion about them. This strategy is used when configuring Internet firewalls; for example, in ZoneAlarm, the default configuration is obtained by analyzing the user answers to a few questions concerning Internet security, connection type and surfing habits. In a similar way, the user is asked to express a value for the privacy sensitivity of each item that could be shared with his mobile, including location, status and mood, address-book, calendar, ring-tones, applications and personal media (photos, videos). User's answers will be encoded as default rule in the Mobile Access Control List (Macl), introduced in the next section. A range of values is used to express how sensitive a piece of information is, including "Highest sensitivity", "High sensitivity", "Medium sensitivity", "Low sensitivity", "No sensitivity". Textual labels are easy to choose for the user, but have a corresponding numerical value used by device. A possible mapping assigns "1" to the "Highest sensitivity and "0" to "No sensitivity", with the other labels having intermediate values in this range.

3.3 User Profile and Mobile Access Control List (Macl)

Once the user has compiled the survey, the application generates the user profile, which consists of public and private sections. The former is a section that can be disclosed to others, while the latter is either hidden or used only by the user for personalization of the application. The most important structure present in the user profile is the Mobile Access Control List (Macl), private table which expresses associations of sharable items (columns) and rules connected to perceived privacy

sensitivity values (rows). As the access control list (Acl) used in computer systems, it maintains and controls access privileges to certain actions. In this case, the actions are related to sharing contents between end users in mobile context.

A Macl (Fig.1) consists of three types of rules: default, contact and context. Only the first one, which is created with the user's answers to the survey, is mandatory. In that case, the same privacy settings are applied to all users and in any context. To achieve higher personalization, additional lines can be added for each of the contacts present in the address-book or for specific contexts. As logical expressions, rules might become very complex when more parameters are involved.

Rule Type	*Label*	*Location*	*Status*	*Mood*	*...*	*Personal Media*
Default	Default	Highest.	Low	Low	…	Medium
Contact	Name1	High	High	High	…	High
…					…	
Context	AtWork	Highest	Low	Low	…	High

Fig.1. Example of Mobile Access Control List (Macl)

A Macl is updated either by manual user interventions or automatically by the system, by using probabilistic models based on user communication and history of past interactions with the system. As one of our initial goals was to reduce the time and effort required to the user when granting sharing permissions, one might observe that the specification of context rules and privacy sensitivity values for each contact present in the address-book might even require a higher workload for the user. Once again, it is a matter of finding a good compromise between quality of results and user intervention. Of course, manual specification of rules and settings requires additional work, but also produces more reliable results. However, average users are usually happy with the default configuration, which requires only the initial effort of answering to a short survey. One additional means for improving trust would require that each time a person is using somebody else trusted information, the original owner should be notified or asked for permission to use that information. This kind of disclosure policy would create symmetric privacy situations, similar to the ones often happening in face-to-face communication.

4 Conclusion

In this article, we introduced a conceptual model for dealing with privacy in MoSoSo applications. Even if human social behavior and mobile context are complex phenomena, automatic support of the user decision making is in some cases a desirable feature. Already today, the need of privacy management mechanisms is perceived as important, but in the near future it will become essential. Through agent technology, ubiquitous services will access and exchange personal data on behalf of the user. Mobile access control lists and privacy management mechanisms could become a key component of ubiquitous services, leaving the control and decision to the user. Without that kind of support, the number of daily decisions could easily become unmanageable for the average user. For example, let us consider the problem

of spam emails; in the early days of the Internet, users were not worried about spam, although it existed in several forms. After a few years, it became one of the most serious Internet problems. Today, a full solution to the problem has not been found, but spam filters have become an essential feature of email systems. In a similar way, privacy management mechanisms could ensure a wider adoption of mobile social software. Future work includes the design of the optimal survey for the generation of the user profile and an evaluation of the proposed approach.

References

1. Agre, P.: Changing Places: Contexts of Awareness in Computing. Human-Computer Interaction. 16(2-4), (2001) 177-192.
2. Anderson, C., Srivastasva, S. Beer, J. Spataro, SE. & Chatman JA. Knowing your place: Self perceptions of status in face-to-face groups. Journal of personality and social psychology (2006), 1094-1110.
3. Babin, B.J., Darben, W.R., Griffin, M.: Work and/or Fun: Measuring Hedonic and Utilitarian shopping value. Journal of Consumer Research, 20(1), (1994) 644-656.
4. Bellotti, V., Sellen, A.: Design for Privacy in Ubiquitous Computing Environments. In Proc. ECSCW'93, (1993) 77-92.
5. Davis, F.D., Bagozzi, R.P., Warshaw, P.R.: Extrinsic and Intrinsic Motivation to Use Computers in the Workplace. Applied Social Psychology 22(14), (1992) 1111-1132.
6. Eagle, N., Pentland, A.: Social Serendipity: Mobilizing Social Software. IEEE Pervasive Computing, Special Issue: The Smart Phone. (2005) 28-34.
7. Farnham, S., Portnoy, W., Turski, A., Cheng, L., Vronay, D.: Personal Map: Automatically Modeling the User's Online Social Network. Interact '03, (2003) 567-574.
8. Goffman, E.: The Presentation of Self in Everyday Life. Doubleday, Garden City, New York, (1959).
9. Langheinrich, M.: Personal Privacy in Ubiquitous Computing. Ph.d. Thesis, (2005).
10. Lugano, G.: Understanding Mobile Relationships, Workshop on Human-Centered Technology, (2006).
11. Lugano, G., Kyppö, J., Saariluoma, P.: Designing People's Interconnections in Mobile Social Networks, I International Conference on Multidisciplinary Information Sciences and Technologies, (2006).
12. Moreno, J.L.: Who Shall Survive? Fundations of Sociometry, Group Psychotherapy, and Sociodrama. Beacon House, (1977).
13. Persson, P., Younghee, J.: Nokia sensor: from research to product. Designing for User eXperience, San Francisco, California, (2005).
14. Preibusch, S. Personalized Services with Negotiable Privacy Policies. CHI 2006 Workshop on Privacy-Enhanced personalization, Montréal, Canada, (2006).
15. Raento, M.: Kill your personal data dead. MobileHCI 04 Workshop on Location Systems Privacy and Control, (2004).
16. Raento, M., Oulasvirta, A.: Privacy Management for social awareness applications. Context Awareness for Proactive Systems (CAPS), (2005) 105-114.
17. Seigneur, J-M., Jensen, C.: Trading Privacy for Trust. 2nd International Conference on Trust Management, (2004).