Analyzing Use of Privacy Policy Attributes in a Location Sharing Application

Eran Toch, Ramprasad Ravichandran, Lorrie F. Cranor, Paul H. Drielsma, Jason Hong, Patrick G. Kelley, Norman Sadeh, and Janice Y. Tsai
Carnegie Mellon University
Pittsburgh, PA
eran@cs.cmu.edu, rravicha@cs.cmu.edu, lorrie@cs.cmu.edu, paulhd@cs.cmu.edu, jasonh@cs.cmu.edu, pkelley@cs.cmu.edu, sadeh@cs.cmu.edu, jytsai@andrew.cmu.edu

ABSTRACT

Privacy in location sharing applications is particularly important due to the sensitivity of users' geographical location. Privacy in most location sharing applications is provided through relatively simple functionality where users have to specify which friends they are willing to share their location with. This approach may not be adequate to fully express users' privacy requirements. In this short article, we present results obtained with a privacy preserving location sharing application, where users are given the option of specifying location disclosure preferences that reflect recurring scenarios, using attributes such as days of the week, times of the day or specific locations. Our results indicate that, while many users tend to start with relatively simple policies similar to those they could specify using today's applications, over time they seem to increasingly refine these policies and take advantage of time and location restrictions.

1. INTRODUCTION

Over the last few years, location sharing technologies have become increasingly pervasive. However, they raise serious concerns about privacy implications [2]. Commercial location sharing applications such as Google Latitude, Yahoo Fire Eagle, and Loopt, offer a coarse control over privacy in which users specify with whom they are willing to share their location with. However, it is doubtful whether this mechanism is expressive enough to support real-world scenarios such as disclosing location to colleagues during work hours and to friends during the evening. Existing research had supported this notion, showing that mechanisms that offer more fine-grained control increase user satisfaction in the location sharing domain [1].

Locaccino[1] is a Facebook-based location sharing application developed by our group. In Locaccino, users are given the option of specifying attributes, including days of the week, times of the day and locations in which they are willing to disclose their locations to others. The results presented herein are based on a live pilot of Locaccino. The pilot was conducted over a period of 6 weeks and involving a total of 131 users.

Our results indicate that, while many users tend to start with relatively simple policies similar to those today's applications offer, over time they seem to increasingly refine these policies and take advantage of time and location restrictions moving towards rules of the type "My classmates can only see my location during 8am and 6pm on weekdays, and only when I am on campus". These results not only suggest that there is an important need for richer privacy settings than currently offered in the marketplace, but also that short-term studies in this domain may fail to capture the richer privacy preferences that emerge over time.

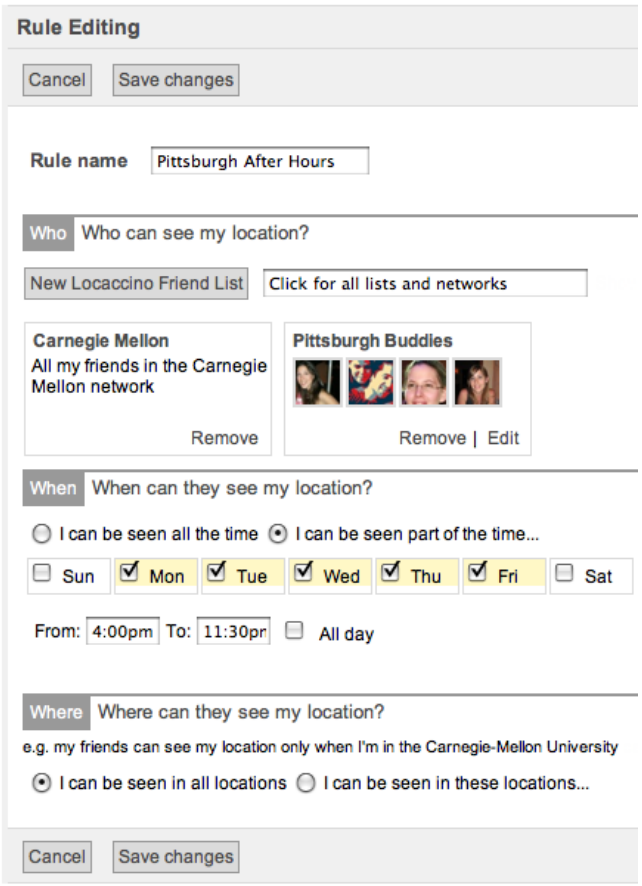

Figure 1: Privacy rules user interface, depicting a rule that includes a time restriction and two friend restrictions (Facebook network and a friend list)

[1]http://locaccino.org

2. PRIVACY SETTINGS IN LOCACCINO

Users control their privacy in Locaccino by setting a privacy policy that consist of a set of rules, which are evaluated when a friend requests the user's location. Figure 1 depicts the user interface used to express the rules. Each rule optionally contains three types of restrictions: a) The friends who can view their location; b) The time frame in which this rule will apply; c) The user's location when the rule applies. Choosing the set of users is done either by creating a friend list or by selecting a Facebook network (e.g., all friends from Carnegie Mellon Students). The user's location is determined using software installed on the user's portable computer. The software determines the location by looking up the nearest set of wireless network access points in Skyhook Wireless' database or in an internal Carnegie Mellon campus database.

3. RESULTS

All privacy policies presented in this analysis were specified by users who used the system for at least 6 weeks, had at least one friend using the system, and were actively using the system to look for their friends ($n = 131$)[2].

About 30% of the rules have no restrictions, allowing all friends to view the user's location at times and all locations. The remaining rules have some type of restriction. The proportions and overlap between restriction types is depicted in Figure 2. About 60% of the rules with restrictions have a friends-based restriction. Of this group, 70% are based on friend lists and 30% are based on Facebook networks. Time and location restrictions are prevalent in 22% and 17% of the restricted rules, respectively.

The majority of rules are created when users begin to use the system and create their privacy policy. However, in the days and weeks after joining Locaccino, users adjust and refine their privacy policies mainly by adding time and location restrictions. Figure 3 depicts the number of changes, i.e. creating and updating rules, according to the time since joining the system. For example, the column *Day 1* represents the number of changes at the first day of usage, column *Week 1* represents the number of changes from the second day to the seventh day, and so fourth.

The proportion of friends-based restrictions relatively to the overall number of changes drops from 62% on the first day, to 52% during the first week and then to 32% during the second week. After the third week of usage, the rate of changes decreases dramatically, and the proportion of friends-based restriction increases. These results were found to be statistically significant according to a paired Wilcox test ($p = 0.02$). Overwhelming majority of friends-based changes involve adding friends who recently joined Locaccino to existing groups or restructuring groups. We rarely find cases in which friends were removed from existing groups.

4. CONCLUSIONS

The results in this short article suggest that there is a significant need for richer privacy settings than currently offered by commercial location sharing applications. Furthermore, these results show that short-term studies in this domain may fail to capture the richer privacy preferences that emerge over time. The results presented here are preliminary, and further studies are being conducted in order to provide additional insight into the results.

[2]All users in this pilot had access to the same functionality, but they did not necessarily start using the system at the same time.

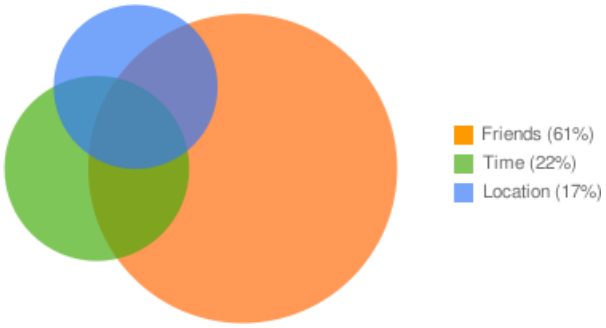

Figure 2: Proportions and overlap between restrictions

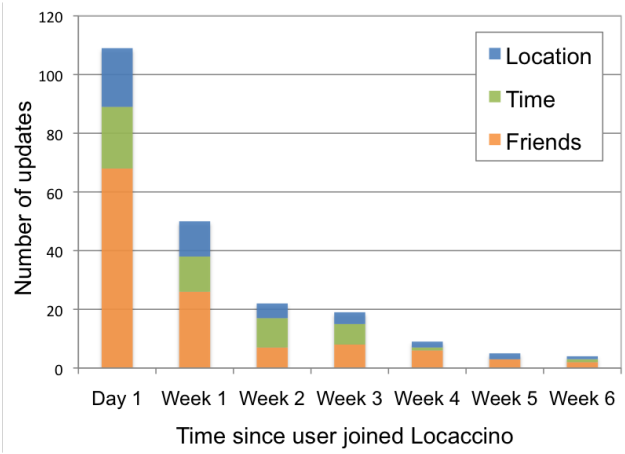

Figure 3: Changes to the privacy policy since the user joined Locaccino

5. ACKNOWLEDGMENT

This work is supported by NSF Cyber Trust grant CNS-0627513 and ARO research grant DAAD19-02-1-0389 to Carnegie Mellon Universitys CyLab. Additional support has been provided by Microsoft through the Carnegie Mellon Center for Computational Thinking, FCT through the CMU / Portugal Information and Communication Technologies Institute, and through grants from France Telecom and Nokia.

6. REFERENCES

[1] Michael Benisch, Patrick Gage Kelley, Norman Sadeh, Tuomas Sandholm, Lorrie Faith Cranor, Paul Hankes Drielsma, and Janice Tsai. The impact of expressiveness on the effectiveness of privacy mechanisms for location sharing. Technical Report 08-141, Carnegie Mellon University - ISR, 2008.

[2] Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 2009.