Too much Information! User Attitudes towards Smartphone Sharing

Alina Hang, Emanuel von Zezschwitz, Alexander De Luca, Heinrich Hussmann
Media Informatics Group, University of Munich (LMU)
Amalienstr. 17, 80333 Munich, Germany
{alina.hang, emanuel.von.zezschwitz, alexander.de.luca, hussmann}@ifi.lmu.de

ABSTRACT

Modern smartphones carry a huge amount of sensitive data. This includes personal information, business information or account information of various online services. In a situation where sharing the device with another person is unavoidable, this data might be in danger. In this paper, we present insights into up-to-date mobile device sharing behavior. We analyzed which data people are concerned of, which data people are willing to share and with whom people would share their device. Our results are based on the findings of a focus group and a user study. Based on those, we derived design implications, which can guide or help with the development of privacy-respectful sharing concepts for smartphones.

Author Keywords
Mobile devices, security, privacy, device sharing.

ACM Classification Keywords
H5.2 [Information Interfaces and Presentation] User Interfaces – User-centered design.

General Terms
Design, Human Factors, Security.

INTRODUCTION

With the emergence of smartphones, mobile devices turned into small personal computers, used for all kinds of applications, ranging from communication devices (e.g. email, text messaging, call functionality) to entertainment applications (e.g. music, games). According to Böhmer et al. [1], who collected usage data of 4,125 participants and 22,626 applications, communication is still the main use case for smartphones, closely followed by content-based services like Internet surfing and social media applications (e.g. Facebook). Nielsen's Mobile Media Report [8], which is a monthly survey of 25,000 mobile consumers in the U.S., supports these results. As content-based applications are prone to store and access a variety of sensitive user data, the smartphone is transformed into a personal storage device. On top of that, the multitude of possible use cases provides additional motivations for users to share their device with others [3]. Given that authentication mechanisms did not evolve, but are still following an all-or-nothing approach, privacy and security issues arise as the smartphone owner is forced to share all data stored on the phone even if she wants to restrict the access to certain features.

Only little research has been conducted to support privacy-respectful mobile device sharing. In 2004, Stajano [7] postulated a "perfect authentication [which] […] could always tell, with absolute reliability and without the user having to do anything, who is currently holding [the device]" to restrict access to sensitive data in shared scenarios. In 2005, Consolvo et al. [2] analyzed the users' sharing behavior according to location-disclosure and found out that the willingness of sharing sensitive information is strongly influenced by the social relation and the current situation. In 2009, Karlson et al. [3] interviewed 12 smartphone owners and revealed that even though users' are concerned about their sensitive data, especially when the phone is out of sight, sharing often cannot be avoided. Their results show, that sharing behavior differs among smartphone owners and depends on the persons the smartphone is shared with. In most cases, device sharing happens spontaneously.

Beside context-aware privacy solutions (e.g. [6]), which focus on the user's surrounding area to prevent shoulder surfing, only few practical approaches have been published to date. In 2009, Liu et al. [4] implemented a concept, called xShare, which is based on user-defined profiles. Each time the mobile device is shared, the fitting profile has to be set explicitly by the owner. Consequently, xShare cannot prevent unintended device sharing and requires additional effort of the user. In [5], a similar approach is presented, where different user types are granted different permissions.

In this paper, we present a two-tired approach. Firstly, we conducted a focus group on smartphone sharing behavior. We then carried out a user study utilizing paper prototyping and interviews to refine the findings of the focus group and to get insights into the required granularity of authentication mechanisms and interaction concepts. Furthermore, we focused on the type of data being shared and analyzed the situations, in which sharing takes place.

We contribute to the field of privacy-respectful device sharing by giving an up-to-date overview of user device

NordiCHI '12, October 14-17, 2012 Copenhagen, Denmark
Copyright © 2012 ACM 978-1-4503-1482-4/12/10... $15.00"

sharing behavior. Since the last analysis in 2009 [3], the market-share of smartphones grew and the devices implemented more data intensive feature. We assume that this progress also changed the way people share their devices.

In the following, we will describe the design and the results of a focus group and a user study, which depict the current state of smartphone sharing behavior. Based on our findings, we provide design implications, which will help the community to develop devices which are usable and support privacy-respectful device sharing in a seamless manner. Finally, the paper is concluded by a brief discussion about the results.

FOCUS GROUP

We conducted a focus group to get more insights into mobile device sharing practices and sharing concerns. The focus group consisted of free discussions with guided questions. We asked participants about the reasons they own a smartphone and if they share their devices. In addition to device sharing, we were particularly interested in their privacy concerns and how sharing takes place. Participants were encouraged to freely express their opinion. The focus group lasted for about 70 minutes.

Seven participants (aged 22 – 27, two female) took part in the focus group. All of them owned a smartphone. Four had an iPhone, two used Android devices and one owned a device with Bada OS.

FOCUS GROUP RESULTS

Access to the Internet was one of the main reasons for our participants to own a smartphone. It allows access to a variety of communication services like Twitter or e-mail while on the go. Smartphones were considered all-in-one devices, providing a rich set of different functionalities that may be at stake when sharing smartphones with others.

In general, participants distinguished between two situations – those in which sharing was initiated by the device owner and situations in which the borrower takes the initiative. The described situations were mostly of spontaneous nature and often coupled to certain functionalities. For example, borrowers should only be allowed to read, but no to write e-mails.

Regarding the timespan of smartphone sharing, participants stated that this was restricted to a couple of minutes. Even then, risks like the sudden appearance of push notifications remain which may reveal personal information to others. Therefore, participants could not imagine sharing their device over days or weeks due to the lack of possibilities to control how the device is used and which data is accessed by the borrower.

Above all, participants were concerned about intentional and unintentional changes by the borrower. For example, intentional changes are the abuse of access to social networks. Unintentional changes comprise the deletion of data, changing of important settings, etc. The mentioned concerns are not equal for each borrower, but depend on the trust level to the borrower. While participants fear theft when sharing their device with strangers, they were more concerned about unwanted data revelation when sharing with friends.

This attitude is also exhibited while sharing their smartphone. There are borrowers which they stay close to in order to observe the interaction with their device and to intervene if necessary. However, there are also borrowers, whom they trust and would leave alone with their device. Sharing attitudes are different among participants and depend strongly on whom they share their device with.

The results of our focus group support findings reported in previous work [3] and also produced new results that helped to broaden our view on the topic. The main results can be summarized as follows:

1. Device sharing is spontaneous and based on different motivations. There is no way to say in advance, why, how and with whom sharing will take place. Furthermore, it can be initiated by the device owner (Push Sharing) or the borrower (Pull Sharing) and is often limited to certain features.
2. Device sharing is strongly app-related and data-related. That is, users want to be able to share applications or restrict access to them as a whole or in part. They also want to allow/restrict access on highly granular levels (e.g. share photo A with person B or only certain functionality of an app).
3. Privacy needs are very subjective. Information that is non-personal for one person might be private for another. Thus, different security levels from "just me" to "anyone" should be supported.
4. Sharing concerns depend on whom they share their device with. Depending on their level of trust, smartphone owners stay close to the borrower to observe their smartphone interaction or even leave the room, if their trust level is high enough.
5. Sharing concerns are not only related to privacy issues, but also to security issues. Smartphone owners are not only concerned about revealing private information stored on their smartphone, but they are also afraid of intentional (e.g., writing text messages in the name of the owner) and unintentional changes (e.g., deletion of content, changes in app settings) by the borrower.
6. Social implications may arise, for instance, if borrowers can see which features the owner is not sharing with them. Push notifications are also a source for privacy infringements. Borrowers may find themselves in an uncomfortable situation, where they read information, that they do not want to see in order to respect the smartphone owner's privacy.

USER STUDY

The focus group revealed that device sharing is strongly app-related and data-related. Thus, we conducted a user study to understand which applications and application features users would share with which group of contacts and how detailed they would differentiate between an application and its features.

The study consisted of 18 semi-structured interviews in combination with paper prototyping sessions. Each interview took about 60 minutes. To base the evaluation on real usage data, participants were asked to bring their smartphones along with them.

Participants were shortly briefed about the study goals. Then they had to complete two counterbalanced tasks. In one task, participants were instructed to browse the contact list of their smartphone and group their contacts with respect to privacy concerns using index cards (see figure 1). Once they were finished, they had to think of additional groups they would share their device with.

In the other task, participants browsed the applications on their smartphone and identified the applications or respective features they use most frequently. Hereby, features are considered as all functionality available inside an application (e.g. messaging is a feature of the Facebook application). Participants wrote down each application and feature on post-it stickers. They also rated them with respect to privacy and security concerns when sharing their smartphones with others. Participants then took the post-its and assigned them to a group, in case they would share these applications/features with it. Post-its were replicated when assigned to multiple groups.

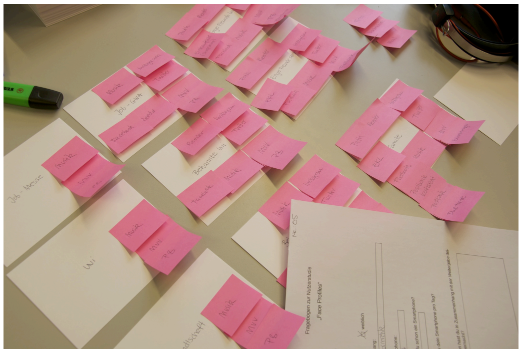

Figure 1: Assignment of applications and application features (pink post-its) to groups (white index cards) by one participant.

The semi-structured interview was closed by a questionnaire covering demographic information as well as smartphone-related questions.

18 smartphone owners, seven female, took part in the user study with an average age of 28 years (20 - 56). Most of them were students and had smartphone experience of two years on average and two hours average use per day. Nine of them owned an iPhone, five an Android phone. The remaining ones used other smartphone models.

RESULTS

Experiences with Smartphone Sharing

When asked about their general experiences with sharing their smartphones, four participants stated they had made negative experiences. This happened either intentionally or unintentionally, including changing phone settings, abusing accounts or writing text-messages. Unintentional changes, for instance, were found on Amazon.com, which changed recommendations based on the searching behavior of the borrower. However, those past negative experiences did not refrain them from sharing their device.

All but two participants noted that they already had shared their smartphone with another person. As mentioned before, out of them, four had made negative experiences when sharing. This strengthens our claim for a secure and privacy-respectful device sharing approach.

Contact Grouping

On average, participants grouped the people they would share their smartphone with into five different groups. The minimal number of groups was four. The maximal number was ten. The five that were named most often were *Friends*, *Family*, *Acquaintances*, *Myself* and *Colleagues*. The groups were clustered by direct quotes of the participants (see figure 2). In general, the transition between groups is seamless. Most of the time, members of a group were assigned based on their logical or social relationship.

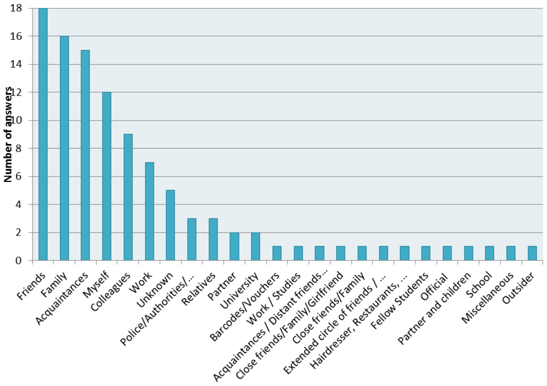

Figure 2: Overview of the different groups assigned by participants for contacts in their contact list.

Most used Applications or Application Features

The most used applications and features can be categorized as *communication* (e.g. mail, call.), *organization* (e.g. calendar, contacts), and *social media* (e.g. Facebook, Foursquare). Regarding the criticality of applications, e-mail, notes, contacts, photos and text messages were considered as more critical than timetables, web browsers or camera apps (see figure 3).

When asked for the most frequently used applications and features, altogether, 124 different ones were mentioned. The average per participant was 14. 41 (68%) unique applications were shared as a whole while 19 (32%) were subdivided into different application features. That is, for 32% of the applications, their sub-features played an important role in sharing decisions. In such cases, the device owner would only like to grant access to specific parts of the application. The importance of configuring application features was strongly user-dependent.

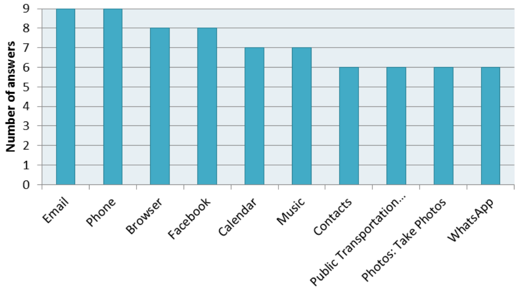

Figure 3: Overview of the top 10 most frequently mentioned applications and application features.

Assigning Applications and Features to Groups

On average, participants assigned eleven applications/features to each group. Each group was assigned at least one application/feature. The group *Family* was assigned most with 81 unique applications/features mentioned for this group. It is followed by *Friends* with 70 and *Colleagues* with 47 unique applications/features. The assignment of applications or application features to a group varied among participants. For example, while some participants allowed friends to use browser applications as a whole, some participants restricted the use of the browser to a limited functionality, like entering a URL to open a website. This indicates the different needs the users have when sharing their smartphone.

IMPLICATIONS AND LIMITATIONS

Our findings support the claim that current all-or-nothing sharing approaches are not sufficient to address the needs when users share their smartphone. Based on the reported findings, we propose the following implications when designing new sharing concepts on smartphones:

1. Sharing concepts have to adapt seamlessly the moment the borrower gets into possession of the device to support the spontaneous nature of smartphone sharing.
2. Sharing concepts have to be transparent to the user in order to avoid social implications.
3. Push notifications have to be hidden when sharing the device in order to avoid unintended revelation of private information.
4. Sharing concepts have to be dynamic, allowing individual privacy settings and preferences to accommodate the different needs of smartphone owners.
5. Rights management should be considered on application level as well as on the level of different features provided within an application.

Since the participants of our focus group and user study were mainly students with a western background, sharing needs of other person groups (e.g. business persons) and sharing practices in countries with different cultural background may be different. Furthermore, we did not actually observe participants in sharing situations, but relied on their self-report during the focus group. These are things that have to be taken into account when designing sharing concepts on smartphones.

CONCLUSION AND FUTURE WORK

The findings have shown that smartphone owners still have many concerns and needs when sharing their device with others. Our findings confirm the results reported in [3]. Sharing behavior has not changed fundamentally in the past few years, but new features found on smartphones have led to new privacy concerns, e.g. push notifications.

The results highlight, that current privacy-concepts are not sufficient. In particular, new concepts have to be created that take the above findings into account. In future work, we want to take these findings and the presented implications to design concepts for smartphone sharing that go beyond the all-or-nothing approach and we want to encourage others to do the same.

ACKNOWLEDGMENTS

This work is partially funded by a Google Research Award.

REFERENCES

1. Böhmer, M., Hecht, B., Schöning, J., Krüger, A., Bauer, G. Falling asleep with Angry Birds, Facebook and Kindle: a large scale study on mobile application usage. In Proc. Mobile HCI 2011.
2. Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P. Location disclosure to social relations: why, when, & what people want to share. In Proc. CHI 2005.
3. Karlson, A.K., Brush, A.J.B., Schechter, S. Can I Borrow Your Phone?: Understanding Concerns when Sharing Mobile Phones. In Proc. CHI 2009.
4. Liu, Y., Rahmati, A., Huang, Y., Jang, H., Zhong, L., Zhang, Y., Zhang, S. xShare: supporting impromptu sharing of mobile phones. In Proc. MobiSys 2009.
5. Ni, X., Yang, Z., Bai, X., Champion, A.C., Xuan, D. DiffUser: Differentiated User Acces Control on Smartphones. In Proc. of MASS 2009.
6. Seifert, J., De Luca, A., Conradi, B., Hussmann, H. Treasurephone: Context-sensitive user data protection on mobile phones. In Proc. of Pervasive 2010.
7. Stajano, F. One user, many hats; and, sometimes, no hat - towards a secure yet usable pda. In 12th Int. Security Protocols Workshop, 2004.
8. The Nielsen Company: State of the Media: The Mobile Media Report (Q3), 2011