Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 109C (2017) 100–107

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Ambient Systems, Networks and Technologies (ANT 2017)

Control yourself: on user control of privacy settings using personalization and privacy panel on smartphones

Yun Zhou[a,*], Marta Piekarska[b], Alexander Raake[c], Tao Xu[d], Xiaojun Wu[e], Bei Dong[e]

[a]*School of Education, Shaanxi Normal University, Xi'an, 710062, P.R.China*
[b]*Security in Telecommunications, Telekom Innovation Laboratories, Technische Universitat Berlin, Berlin, 10623, Germany*
[c]*Audiovisual Technology Group, Institute for Media Technology, University of Technology Ilmenau, Ilmenau, 98693, Germany*
[d]*School of Software and Microelectronics, Northwestern Polytechnical University, Xi'an, 710072, P.R.China*
[e]*Key Laboratory of Modern Teaching Technology, Ministry of Education, Shaanxi Normal University, Xi'an, 710062, P.R. China*
[f]*School of Computer Science, Shaanxi Normal University, Xi'an, 710119, P.R. China*

Abstract

The paper assesses the gap between actual and perceived privacy features of smartphones, exploring privacy as one decision-making factor in information protection, and the balance between privacy control and the required user interaction with the settings. We conducted a fine-grained evaluation partly based on the Privacy Panel, a protection solution on Firefox OS including features of Find my Device, Backup, Location Blurring, and Guest Mode. Results showed that safety as one decision-making factor impacted information protection in different use cases at different levels. Although people sacrifice more privacy as the price of a handset grows, they still see privacy as a factor of various significance with respect to context of finding back smartphone and selecting storage places. People were satisfied to use improved privacy settings but still did not well adapt to complex personalized interfaces. Sorting methods, recommendations and establishing profiles have shown to be feasible ways to assist users to balance between full control and the additional interaction burden when adjusting privacy settings in a complex app ecosystem.

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.

Keywords: Privacy; Smartphone; Control; Personalized Settings; Lab Study

1. Introduction

Although privacy is by no means a new issue for users, it becomes increasingly important and complex when intertwining with mobile computing. As smartphones have growingly integrated into people's lives, especially since 2012, user activities associated with mobile devices naturally produce a larger amount of personal information. This trend gives rise to unavoidable privacy and security risks at different levels. Many prior studies have focused on tools to deliver over-advanced privacy control to users. However, the existing schemes for privacy protection on smartphones

* Corresponding author. Tel.: +86 29 85308047 ; fax: +86 29 85308047; Email: zhouyun@snnu.edu.cn.
E-mail address: zhouyun@snnu.edu.cn

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.05.300

typically do not provide users with sufficiently personalized but easy-to-use choices to control their privacy settings. Generally, a user is required an in-depth understanding and considerable effort to achieve the fine-grained control, and suffers from an even heavier burden when the number of apps increases. Although there are a handful of studies that investigate usability of new privacy control models beyond all-or-nothing settings, we are still unclear about users' perception and the burden of interaction when they set complex privacy settings in an app ecosystem. In addition, to achieve a better understanding of the design of usable access control on smart devices, it is essential to know how a user configures settings to make privacy decisions. Our goal is to explore the aforementioned issues and support users to accommodate improved privacy protection on smartphones.

In this paper, we first briefly present Privacy Panel, containing protection features like Find My Device, Backup, Location Blurring and Guest Mode. To explore the users' attitudes and behaviors towards personalized control of privacy protection in an app ecosystem, we conducted a lab-based user study involving 26 participants. From this user study, we conclude that 1) Safety as one decision-making factor impacted information protection in different use cases at different levels. Although participants sacrifice more privacy as the price of a handset grows, they still see privacy as a factor of various significance with respect to context of finding back smartphone and selecting storage places. 2) People were satisfied to use improved privacy settings but still did not well adapt to complex personalized interfaces. Sorting methods, recommendations and establishing profiles have shown to be feasible ways to assist users to balance between full control and the additional interaction burden when adjusting privacy settings in a complex app ecosystem.

2. Related Work

In this section, we briefly summarize the research work related to our exploratory studies. Also, we survey and compare different privacy features on other OSs.

The reviewed literature implies that users are more or less concerned about privacy on their smartphones[1] [2] [3] [4], even though smartphone defies users' privacy expectations to some extent. Results in [1] indicate that users are more concerned about privacy on their smartphones than on their laptops. The qualitative study by Karlson et al.[4] on understanding users' concerns when sharing mobile phones (without control of protection) provided the evidence that users were not comfortable with data privacy, fear of data deletion, carelessness, etc. Thus, people often need to set limits on who could see or use resources, data and apps on smartphone. Moreover, the degree of concern obviously depends on the actual "use case", with smartphone sharing being among those most strongly linked with concerns, and location-based services considered as less problematic. One of alternative solutions to let users take over control to protect privacy is to provide them with a new improved privacy model or mechanism to replace all-or-nothing settings like Android permissions. With Android's all-or-nothing approach during installation, users either accept all permissions or give up privacy completely. Some studies tried to propose and build protection tools like "Apex"[5] and "ProtectMyPrivacy"[6] to deliver privacy control to users and help them keep away from privacy violations. Apex is an extension of Android's permission model, which provides a finer-grained control over permissions and supports the user to impose constraints on the usage of resources. ProtectMyPrivacy is an iOS application, which proposes pop-ups to let the user allow or refuse access from apps and recommends using crowdsourcing. Some research work focus on identifying malicious behavior and monitoring data leakage of apps[7] [8], but without investigating usability of these tools and users perception and reaction when reading such complex information. Achieving fine-grained control means, usually, higher user effort[9] that increases with the number of apps installed. There is a handful of studies that explore that scenario, however few shows the users' perception of the complexity connected to non-binary privacy settings. It is especially important to conduct such research to better inform the design of access control on smart devices that is intuitive, given that privacy is a decision-making factor for settings configuration.

We analyze, compare and label features on other OSs. We found features similar to Find My Device(FMD), Backup(BP), Location Blurring(LB) and Guest Mode(GM) on the latest version of four smartphone OSs: Android OS, iOS, Window Phone OS, and BlackBerry OS. As shown in Table 1, we survey and mark out the availability of four features on OSs, considering different manufacturers. All four OSs have been equipped with features of Find Device and Backup. iOS and Android are equipped with Find My iPhone and Android Device Manager respectively, including both app and online services. Similarly, Windows Phone offers Find My Phone in Settings and online service. BlackBerry only releases an omnipotent tool BlackBerry Protect, which contains remote control features.

Find Device feature and Backup are fundamental function on smartphones. It is undeniable that privacy is a decision-making factor of activities involving personal data. Cloud as a storage place is an option which brings about not only always-available data storage and retrieval, but also the potential risk of leaking stored data. Users often profit from the convenience but ignore the related privacy threat. Although 76% of respondents cited security and privacy as a key barrier to cloud adoption in Cisco's CloudWatch 2011 report [10], unprecedented accessibility of resources of cloud computing attracts users to store their data. We argue that people consider safety at different levels depending on activities, and we analyze these levels in the context of configuration settings regarding Find My Device and Backup in later parts of this paper. To protect location information, users can simply block/unblock GPS location for each app on OSs. However, it is still an all-or-nothing privacy model but refines control at the app level. For example, the user either provides the exact location to the weather app to automatically obtain a local weather report, or blocks this information, but then will not get any location-specific information. In this scenario, it is sufficient to give the app a blurred city location information instead of exposing the exact location. The feature Location Blurring could provide a finer-grained control and a more powerful protection for users. We differentiate *GPS location block* from *Location Blurring*, so that OSs not equipped with *Location Blurring* are indicated with "No". We found that smartphone OSs started to attach more importance to the feature of "Guest Mode" since 2014. For example, Android users can access multiple-user settings and use Guest/Profile/User account types to safely share their smartphone. On iOS, users can define and block several interactive areas in Settings under the category of accessibility individually. In this way, when sharing the smartphone, the owner could explicitly switch to this feature and disable user interface items that he does not want a guest to use. Phone sharing has been proven to be popular among users by prior studies [3 4]. The study [11] conducted a focus group to explore sharing behaviors, covering understanding which data people are concerned of, which data they are willing to share and with whom people would share their device. Also, there are studies that have investigated sharing practices using surveys, interviews, etc [12 13].

Table 1. Privacy features provided by manufacturers on OSs.

Features	Lost or stolen device control	Backup data	Location privacy	Advanced secondary user mode for device sharing
Android	Yes	Yes	No	Yes
iOS	Yes	Yes	No	Yes
WP	Yes	Yes	No	Yes
Blackberry	Yes	Yes	No	Yes
FirefoxOS	FMD	BP	LB	GM

As can be concluded from the survey above, in recent years OS providers have gradually given privacy control of smartphones to the users. In turn, refined control settings increase the users' effort for operating their phones. Thus, it is essential to study how users react on the effort required for making privacy settings, and the implications on their view of privacy when they make respective decisions. Finally, we also want to explore how effective our proposed solutions are, which aim at supporting users to accommodate the app ecosystem.

3. Design and Implementation of Privacy Panel

In this section we briefly describe the design and implementation of the Privacy Panel. We have proposed this solution to give users better control over what is happening to their data. We implemented the Privacy Panel on Firefox OS, a web-based Operating System. We include the developed features into the settings and build on top of some of the existing elements. The Privacy Panel (see Figure 1) contains features *Find My Device*, *Backup*, *Location Bluring*, and *Guest Mode*, but is not limited to these.

Find My Device offers the possibility of locking, tracking, wiping and activating a ringtone on the device. Backup gives the users a choice whom to trust with data, which introduces another improvement in privacy protection. We have created a backup mechanism that allows to choose where the data should be stored. With the Privacy Panel, the user is able to pick the location – be it a default Mozilla server, some popular storage providers, or his personal computer. With respect to Location Blurring, in the Privacy Panel the user can choose the accuracy of the location services on a per-application basis. Turn Location Off allows the user to choose not to give any location data at all. Give Precise Location leaves the system without any changes. Choose a Position allows the user to fix his position

to a set of coordinates. We provide a list of predefined values and a search that allows to find a City or Country (where the coordinates are set to the center of mass of the place). Additionally the user can enter custom latitude and longitude. With Blur by X km, the user can choose a distance, and his position will be randomly selected from a range of X km around his location. The choice is flexible and can vary from 1 to 500 km. The applications installed on the phone carry a lot of information about the owner of the device. Elements under protection of the Guest Mode can be divided into three groups: applications, data and resources. This feature consists of two parts: settings and an activation interface. Users can decide which apps will be not only accessible, but also visible on the phone. After entering the Guest Mode, the apps will disappear from the screen and from the internal search engine. There is a list of pre-defined elements that will always be removed, like settings or the Privacy Panel (since the secondary person using the smartphone should not be allowed to change any options in settings). Upon entering the Guest Mode, the data stored in each of defined elements is substituted with an empty list, just as if no one ever used the phone. Once the phone is handed back to the owner, the original information is restored. The databases include contacts, call history, SMS history, emails, photos, browser history. Lastly there is a possibility of limiting the access to the resources, like WiFi, cellular data, etc.

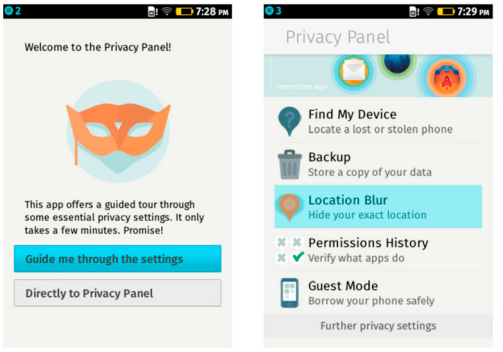

Fig. 1. Overview of Privacy Panel

4. User Study

Privacy Panel provides rich improved control and options, thus we leverage it as the testbed of this user study. We believe that the tool will help reflect the users' privacy attitude and decisions. To obtain a profound understanding on the users' attitudes and behaviors towards personalized control of privacy protection in an app ecosystem, we organized a structured usability lab study of 26 users. We explored the following research questions:

- What is the importance of privacy as a decision-making factor in different contexts related to personal data? The answer is gathered mainly from the evaluation on Find My Device and Backup.
- How do users interact with personalized settings and how do they adapt to the world of full control over the ecosystem? The answer is gathered mainly from the evaluation on Location Blurring and Guest Mode.

We recruited participants from Prometei, a database for recruiting evaluation subjects, and offered 15 euro for participation. Participants didn't need to own a smartphone. Some of them had feature phone but experienced using a smartphone, when they borrowed a device from acquaintances. In total, we had 10 male and 16 female participants. Their ages were distributed between 17 and 55, with the breakdown to: 23.1% in the group 18-24, 46.2% were 23-34 years old, 19.2% between 35-44, and 11.5% belonged to the category 45-54. We conducted 90-minute study sessions and had one participant per session. The main procedure can be presented as follows. Tester greets the participant and asks to fill out the agreement sheet permitting us to use the data and the background survey. Tester introduces the user study and explains the procedure briefly. The participant is asked to fill out questionnaires, explore the features of the phone, learn how to use the Privacy Panel, and set up settings of each feature. Tester thanks the participant and pays the promised amount of money. Each participant learned and performed tasks on one Alcatel phone on Firefox OS. We recorded users' attitudes towards privacy and their choices in the privacy settings.

5. Results and Discussions

To find the answer of the first question, we wanted to see how do users' perceive the cost of privacy. We asked them to choose if, at different price levels, it is more painful for them to lose the phone or the data on the device when it is stolen. As can be seen in the Figure 2, the more expensive the device, the less important the data is. The turning point occurs when the phone price ranges from 301 to 400 euro.

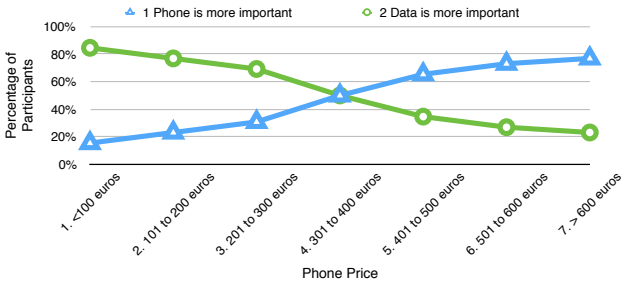

Fig. 2. Participants' relative level of perception of phone importance vs. data importance

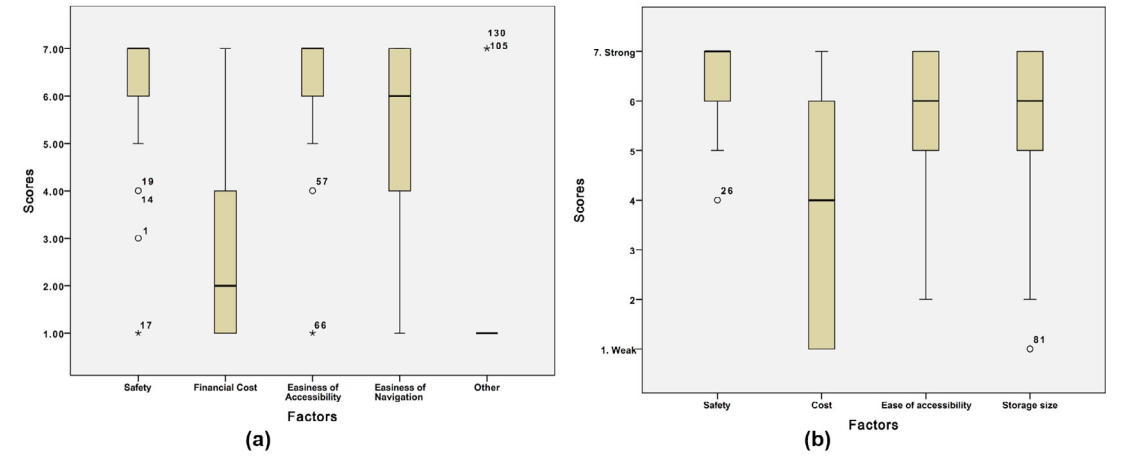

Fig. 3. Scores of factors that impact participants decisions on control methods (a) and storage places (b)

In addition, we asked what are the factors influencing users' decisions on the control methods - why do they choose emails or text messages. The four main reasons we listed were: safety, financial cost, ease of accessibility (ease of connecting Internet or finding a phone to send SMS) and ease of navigation (see Figure 3(a)). Participants were also free to give other arguments in the "other" field. We used the semantic differential technique with paring of "Weak/Strong" to form the answers in a seven-scale. More than 80% participants considered safety and ease of accessibility as strong factors (scores of 5, 6 and 7) impacting their way of controlling smartphone remotely. They gave high scores to safety (Mdn=7), ease of accessibility (Mdn=7) and ease of navigation (Mdn=6). Less than 19% thought costs (like SMS costs) would affect their decisions (Mdn=2). With respect to the storage place of backup, we asked participants how strongly each factor influences their decision. We proposed four potential factors: safety, financial cost, ease of accessibility (For example, cloud can be accessed anywhere at anytime when connecting Internet, but PC not) and storage size. Participants were free to include their own reasons under the category "other". We used the semantic differential technique with paring of "Weak/Strong" to form the answers in a seven-scale. All participants except one considered safety as having a strong impact (scores grater than 4). As illustrated in Figure 3(b), they gave high scores to safety (Mdn=7), ease of accessibility (Mdn=6) and storage size (Mdn=6). About 46.1% said that costs would affect their decisions (Mdn=3.5). Overall, Safety as one decision-making factor impacted information protection in different use cases at different levels. Although participants sacrifice more privacy as the

price of a handset grows, they still see privacy as a factor of various significance with respect to context of finding back smartphone and selecting storage places.

To find the answer of the second question, we mainly used Location Blurring and Guest Mode as the testbed. Prior study [14] discussed users' social behaviors on sharing when they have more location disclosure choices. However, we would like to know how location information would be exposed to apps by users. We make a list of representative and most used apps, which have been selected based on categories from preinstalled apps like browser, and from Firefox marketplace, including games, social networking, video, utility, fitness, etc(see Figure 4). We asked participants to choose different blurring levels depending on each application. First, participants expose location information to apps required location reasonably like Easy Taxi, Run Recorder, AccuWeather. Next, we observed that users were reluctant to give access to apps that had no explicit reason to collect location data such as the Dictionary app. Game apps and social networking apps were refused more by participants to obtain location. Almost less than 25% participants used location blurring features including using random location, blurring by given number of km, and choosing a place. They simply gave no access to location at all. Results from our study also indicated that people were not used to set settings for blurring location at a refined level. They also reported difficulties when using this setting. They reported that "It can get annoying with too many apps if you decide to configure each app manually" and "Too many possibilities and I prefer a few categories (to organize apps)".

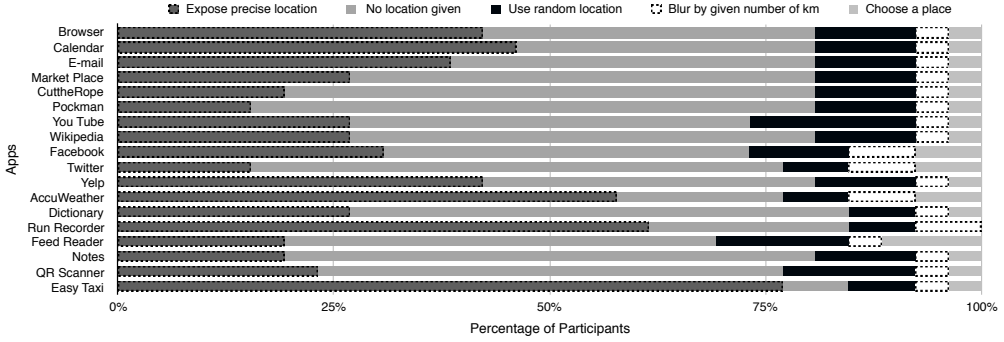

Fig. 4. How participants used Location Blurring to protect location information

We measured users' thoughts on going through all apps to blur location and their opinions on our proposed recommendation scenario. The answer was formed by a seven-point scale of semantic differential technique with paring of "Not worthy/Worthy". Participants gave scatted responses (Mdn=4). The comments from users who gave negative scores showed that it was unnecessary for them to adjust location information for every app: "It would be ok for me to have more choices but not essential", "I would prefer categories like Games, but not each game-app separately", "I prefer one general settings that I would do the same for all", and "I just want to close location information for some apps". However, the positive comments showed that it was essential to have full control over each app to adjust location information, including "I could have full control for each app", "There is a need to have different settings", and "I make a choice from case to case and can set for each app separately".

In app ecosystem, increased personalized controls and management over each app in Settings are provided to users. However, as the number of apps grows, users will suffer a heavier burden of adjusting settings for each application separately. A solution could be the support of sorting mechanisms. Thus, we propose to enable filtering by most used, recently added, recently opened and alphabetical. To verify which methods would be preferred by the users, we asked them to answer on a seven-point scale of semantic differential technique with paring of "Not attractive/attractive". Results showed that mostly used (Mdn=7) and alphabetical sorting (Mdn=6) were the attractive methods. Recently added (Mdn=4) and date opened (Mdn=4) were not well accepted by users. To enhance the user experience, we propose a recommendation mechanism, that would base its predictions on the owner's previous navigation history and categories of apps. The assistant would suggest the right level of adjusting location accuracy in order to reduce the decision burden. For instance, when one would install a new social networking app, a notification would show up and recommend setting of precise location, as previously user set that for other social networking apps. To know how strong user has willingness to have such recommendation engine that assists setting, we asked participants to judge it

on a seven-point scale of semantic differential technique with paring of "1-Weak/7-Strong". Results showed that they would be very willing to use such a system (Mdn=6).

To know how users create profiles for different persons, we asked them to set up Guest Mode for lenders respectively. We proposed actors based on relationships used in xShare [3], however differentiated child (under 18 years old) from others. Thus, we had nine types of lender, including stranger, acquaintance, coworker/classmate, relative, parent, sibling, child, spouse and friend. As shown in Figure 5(a), the x-axis represents percentage of participants, which is separated by three red line into four columns. Each column stands for one resource involving all participants' configurations. We observe that guests can be divided into three groups: stranger, limited trust (acquaintance, coworker/classmate, and child), higher trust (relative, parent, sibling, spouse, and friend). WiFi is the one resource that has been always made available to a guest.

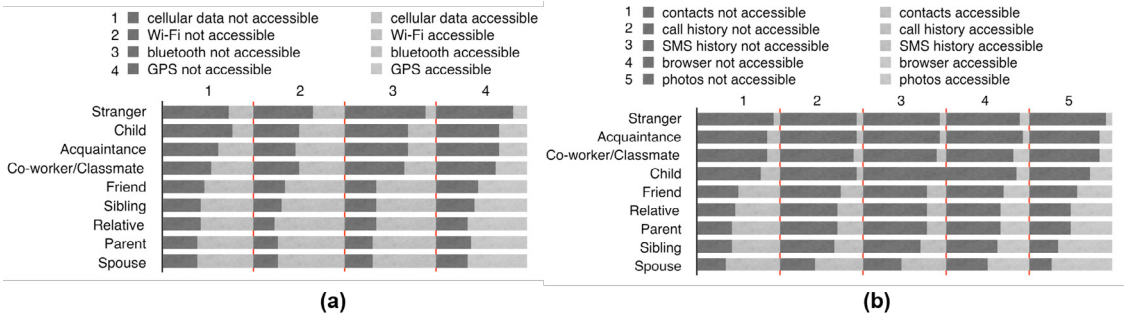

Fig. 5. Percentage of responses on blocking/unblocking resources to nine actors

In Figure 5(b) and 6, we present the decisions on giving access to data and apps to the nine types of actors. Here the guests are clearly divided into two groups: very limited trust (stranger, acquaintance, coworker/classmate, child) and higher trust (relative, parent, sibling, spouse, friend). A few participants were willing to expose their contacts, call history, SMS history, browsing history and photos to people they do not have a strong relationship with as well as their children. Photos tended to be much more protected from strangers. Also calls made and SMSes sent were rarely exposed to them. Similar groups were found when giving access to apps as to data. However, even for guest with whom the owner had strong relationships with, about half of the participants were reluctant to expose the apps that indicated their preferences(such as usage), allowed to control the phone (such as settings), gave access to personal information (such as email, Facebook, Twitter, Notes). For the sorting methods in Guest Mode, users were most interested in having mostly used (Mdn=6) and alphabetical sorting (Mdn=7) methods, while recently added (Mdn=3) and date opened (Mdn=3) were much less accepted by users.

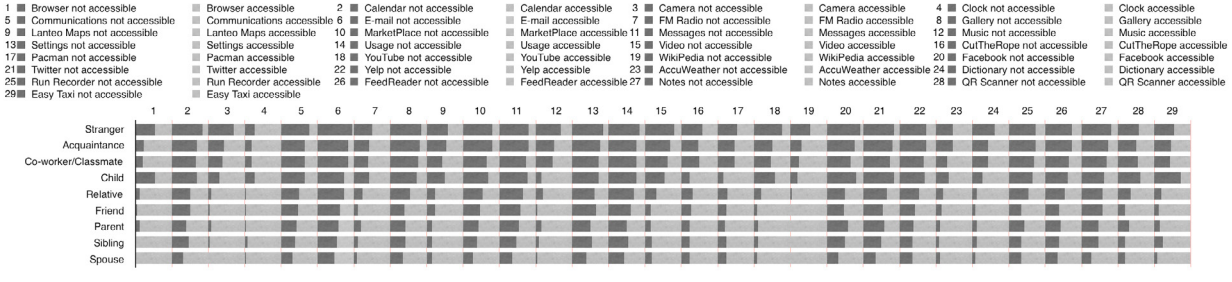

Fig. 6. Percentage of responses on blocking/unblocking apps to nine actors

Finally, We discuss the answers to research questions that are presented at the beginning of the user study. 1) What is the relative importance of privacy as one of the decision-making factors in different contexts connected to personal data? Results from weight of privacy indicated the concern about the data on the phone decreases and the handset becomes more important, as the price of a device grows. Results from the factors influencing users' decisions on the control methods and storage places showed that people strongly keep safety as one high-priority factor when

it is about finding a lost smartphone and selecting places for storing data. Safety as one decision-making factor impacted information protection in different use cases at different levels. Although participants sacrifice more privacy as the price of a handset grows, they still see privacy as a factor of various significance with respect to context of finding back smartphone and selecting storage places. Safety as one decision-making factor impacted information protection in different use cases at different levels. 2) How do people interact with personalized settings and adapt themselves to take over control of privacy on app ecosystem? Overall, results from Location Blurring showed that people were not adapted well to complex personalized interfaces. It is thus hard to identify the common settings for features like Location Blurring or Guest Mode. However, we believe that categories in the Marketplace could reflect the potential impact on privacy. The apps in a given group could then be given similar location privilege access. Moreover, adding sorting methods and recommendations based on previous choices of a user could also provide significant assistance in decision making process, and assist to balance between full control and interaction burden. Results around Guest Mode showed that guests could be clearly divided into groups on exposing resources, data and apps. Different resources except WiFi were almost exposed at the similar level, and access to WiFi is considered a must for everyone. There are clear differences in exposing different data types and applications to users. Overall, sorting methods, recommendation and establishing profiles are alternative feasible ways to assist smartphone users to balance between full control and interaction burden in the app ecosystem.

6. Conclusion

This study is motivated due to missing studies in the field of privacy management. In this paper, we present a fine-grained study to investigate the users' attitudes and behaviors towards personalized control of privacy protection in an app ecosystem. We found that 1) Although participants sacrifice more privacy as the price of a handset grows, they still see privacy as a factor of various significance with respect to context of finding back smartphone and selecting storage places. 2) Sorting methods, recommendation and establishing profiles are alternative feasible ways to assist smartphone users to balance between full control and interaction burden in the app ecosystem.

References

1. E. Chin, A. P. Felt, V. Sekar, D. Wagner, Measuring user confidence in smartphone security and privacy, in: Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM, 2012, p. 1.
2. A. P. Felt, S. Egelman, D. Wagner, I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns, in: Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices, ACM, 2012, pp. 33–44.
3. Y. Liu, A. Rahmati, H. Jang, Y. Huang, L. Zhong, Y. Zhang, S. Zhang, Design, realization, and evaluation of xshare for impromptu sharing of mobile phones, Mobile Computing, IEEE Transactions on 9 (12) (2010) 1682–1696.
4. A. K. Karlson, A. J. Brush, S. Schechter, Can i borrow your phone?: understanding concerns when sharing mobile phones, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2009, pp. 1647–1650.
5. M. Nauman, S. Khan, X. Zhang, Apex: extending android permission model and enforcement with user-defined runtime constraints, in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ACM, 2010, pp. 328–332.
6. Y. Agarwal, M. Hall, ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing, in: Proceeding of the 11th annual international conference on Mobile systems, applications, and services, ACM, 2013, pp. 97–110.
7. Y. Zhou, X. Zhang, X. Jiang, V. W. Freeh, Taming information-stealing smartphone applications (on android), in: Trust and Trustworthy Computing, Springer, 2011, pp. 93–107.
8. W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, A. N. Sheth, TaintDroid: an information flow tracking system for real-time privacy monitoring on smartphones, Communications of the ACM 57 (3) (2014) 99–106.
9. D. K. Smetters, N. Good, How users use access control, in: Proceedings of the 5th Symposium on Usable Privacy and Security, ACM, 2009, p. 15.
10. N. Kshetri, Privacy and security issues in cloud computing: The role of institutions and institutional evolution, Telecommunications Policy 37 (4) (2013) 372–386.
11. A. Hang, E. Von Zezschwitz, A. De Luca, H. Hussmann, Too much information!: user attitudes towards smartphone sharing, in: Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design, ACM, 2012, pp. 284–287.
12. T. Matthews, K. Liao, A. Turner, M. Berkovich, R. Reeder, S. Consolvo, She'll just grab any device that's closer: A study of everyday device & account sharing in households, in: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ACM, 2016, pp. 5921–5932.
13. Y. Zhou, T. Xu, A. Raake, Y. Cai, Access control is not enough: How owner and guest set limits to protect privacy when sharing smartphone, in: International Conference on Human-Computer Interaction, Springer, 2016, pp. 494–499.
14. K. Tang, J. Hong, D. Siewiorek, The implications of offering more disclosure choices for social location sharing, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2012, pp. 391–394.