Received: 30 December 2017 | Revised: 29 March 2018 | Accepted: 22 June 2018
DOI: 10.1002/cpe.4884

WILEY

SPECIAL ISSUE PAPER

User attitudes and behaviors toward personalized control of privacy settings on smartphones

Yun Zhou[1] | Lianyong Qi[2] | Alexander Raake[3] | Tao Xu[4] | Marta Piekarska[5] | Xuyun Zhang[6]

[1]School of Education, Shaanxi Normal University, Xi'an, China
[2]School of Information Science and Engineering, Chinese Academy of Education Big Data, Qufu Normal University, Qufu, China
[3]Audiovisual Technology Lab, Institute for Media Technology, University of Technology Ilmenau, Ilmenau, Germany
[4]School of Software and Microelectronics, Northwestern Polytechnical University, Xi'an, China
[5]Security in Telecommunications, Telekom Innovation Laboratories, Technische Universitat Berlin, Berlin, Germany
[6]Department of Electrical and Computer Engineering, The University of Auckland, Auckland, New Zealand

Correspondence
Yun Zhou, School of Education, Shaanxi Normal University, 199 South Chang'an Road, Xi'an, Shaanxi 710062, China.
Email: zhouyun@snnu.edu.cn

Tao Xu, School of Software and Microelectronics, Northwestern Polytechnical University, 127 West Youyi Road, Xi'an 710072, China.
Email: xutao@nwpu.edu.cn

Funding information
Mozilla Foundation; Telekom Innovation Laboratories; National Natural Science Foundation of China, Grant/Award Number: 61702417 and 61703259; Shaanxi Natural Science Foundation, Grant/Award Number: 2017JM6097; State Key Laboratory for Manufacturing Systems Engineering, Grant/Award Number: sklms2016001

Summary

The fine-grained access control has been proved to be a reliable tool to ensure preserving of privacy of end users. In fog computing, one of the challenges is to understand users' attitudes and behaviors toward personalized control. However, few of studies have given a clear view on users' perception of the burden of interactivity when they set complex privacy settings. To this end, we conducted a user study including a lab study with 26 participants and an evaluation with 223 participants. From the lab study, we found that participants were satisfied with improved privacy settings but did not adapt well to complex personalized interfaces. We proposed effective methods to assist users to balance between the full control and the additional interaction burden, including sorting, recommendations, and establishing profiles. After this lab study, we organized a survey evaluation additionally to explore users' current usage of privacy features. Results from the evaluation showed that the principle reason that users failed to use privacy features was that they were not appropriately aware of these features. A key conclusion is that privacy settings should not only let users take over the control of smartphones but also inform them of the knowledge on privacy practices.

KEYWORDS

access control, fog computing, personalized privacy, smart phone, user study

1 | INTRODUCTION

Many security and privacy issues such as the leakage of personal data, location, usage records, and preference, which traditionally exist in cloud computing platforms, have severely extended to fog computing[1] where a huge number of sensing devices like built-in motion sensors in smartphones, environmental sensors and position sensors are widely developed and deployed. Specifically, companies (trusted or untrusted) are able to record human behavior and collect user data with much higher variety and quantity than ever before in the context of fog computing. The reviewed literature implies that users are concerned about privacy on their smartphones. They want to have control by whatever means they could and the clear

evidence suggested that greater controls would increase trust and engagement with services and apps.[2] Generally, achieving the fine-grained control requires more effort of users[3,4] and they will likely suffer a heavier burden when the number of apps increases. Although there are a handful of studies that investigate new mechanisms beyond all-or-nothing setting choices, we are not clear on users' perception on the burden of interactivity when they set complex privacy settings in the app ecosystem. In addition, to better inform about design of access control on smart devices, it is essential to know how users set settings and how much users expose apps, sensors, and resources for each relationship. This is especially true as privacy is or should be one of the most important decision-making factors when configuring settings. Finally, we also want to explore how effective our proposed solutions are, which aim at supporting users to accommodate the app ecosystem.

To study the users' attitudes and behaviors toward personalized control of privacy protection in an app ecosystem, we conduct a fine-grained user study including a lab study with 26 participants and a survey with 223 participants. In this paper, we first present privacy features that have to be considered, including Find My Device, Backup, Location Blurring, and Guest Mode. From the lab-based user study, we found that participants did not consider all features to be connected to privacy. In particular, the storage of personal information has not been integrated with privacy protection in the mental models of most participants. Safety as one decision-making factor impacted information protection in different use cases at different levels. Based on usage of privacy features, we found that privacy recommendation, use and reuse of profiles, as well as sorting methods are feasible solutions in an app ecosystems to help users adapt to personalized control. Results from the survey indicated the principle reason that users did not use privacy features and their expectation. Finally, we discuss the implications for usable privacy interface design from these results.

The rest of this paper is organized as follows. We outline related work and describe the features to be evaluated in Sections 2 and 3, respectively. We present the user study focusing on issues of privacy settings in Section 4 and results in Section 5. We discuss the results and implications for design in Section 6 and conclude in Section 7.

2 | RELATED WORK

In this section, we briefly summarize the research work related to our exploratory studies. First, we present studies on users' concerns about privacy on smartphone and increased requirements on controlling respective settings. Then, we discuss the research on improved and new control mechanisms instead of all-or-nothing access. Finally, we survey and discuss how the improved privacy control has been involved in OSs. We believe that privacy protection is one of the salient parts and should be included into smartphone OS.

2.1 | Users' concerns about privacy on smartphone and their requirement on control

Chin et al explored user perceptions of smartphone security and their confidence in smartphone privacy by interviewing 60 smartphone users.[5] Results indicated that users were more concerned about privacy on their smartphones than on their laptops, and they worried about data loss, malicious applications, wireless network attackers, etc. Other work like the survey of smartphone users' concerns[6] looked into particular aspects of privacy concerns. This survey asked 3,115 participants to rank risks by levels of their concern and found, as one of the results, that revealing their location is not a high-ranked user concern. Personal data leakage could lead to not only concern but also other negative emotions. In the work of Shklovski et al,[7] the authors conducted two studies involving smartphone users in Western European countries, including a semi-structured interviews with 13 participants and a survey with 272 respondents. The motivation was to explore perceptions of privacy and mobile app use. Many of findings from this study confirmed other studies of attitudes toward smartphone data leakage and privacy. Results also showed that data collection elicited negative feelings of users like being uncomfortable, being deceived, and being violated in "creepy" ways. In addition, phone sharing behaviors are proven to be popular at different levels among smartphone users and feature phones users who live in the smartphone world.[8-10] The study by Hang et al[11] conducted a focus group to explore sharing behaviors, covering understanding which data people are concerned of, which data are willing to share, and with whom people would share their device. In addition, there are studies[12,13] that have investigated sharing practices using surveys, interviews, etc. The work of Liu et al[8] provided results from an international interview including 60 participants from China, South Korea, Iran, and the USA, which showed that phone sharing is popular and involves a wide range of applications, reasons, social settings, and relationships. The qualitative study by Karlson et al[9] 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.

Privacy control and data leakage from smartphone should no longer be ignored with the broad use of smartphones. Many prior studies on privacy control analyzed privacy settings in online social networks, including measuring the disparity between the desired and actual privacy settings,[14] mismatch between perceived, preferred, and actual settings,[15] or the important role of privacy settings at large.[16] The research on the users' perspective on mobile privacy conducted by Futuresight for the Groupe Speciale Mobile Association, GSMA[17] explored precautions taken, perceptions of control, and desire for control overall, conducted in the UK, Singapore, and Spain. Results showed that the majority of users felt more in control of their personal information when using a PC than when using a mobile. However, most users were not really sure how much in control they were of mobiles. Overall, users call for more control on their smartphones and tablets.

2.2 | Beyond all-or-nothing setting choices

Although users have concern and negative feelings on privacy leakage, their attitudes and behaviors indicated that existing privacy mechanisms and settings are not successful to inform or assist them to protect their privacy adequately. Previous studies have focused on users' attitudes and behaviors toward privacy protection based on analyzing Android permissions, location sharing, and phone sharing. Felt et al[18] conducted an internet survey and a lab study to determine if Android's permission system is effective at warning users. Results showed that participants paid little attention to permissions, and some participants did not readily understand the meaning of "permissions," which may hinder users to take proper decisions while downloading apps. The "PrivacyFacts" research by Kelley et al[19] found that, although users did not use the current Android permissions display, if permission information was presented to them in a clearer way, their decisions could be influenced and privacy would become a strong decision-making factor. TreasurePhone[20] proposed an approach, which supports context-dependent data privacy and enables users to manually switch between different contexts. In this way, users were not limited to use the simple privacy model that only distinguishes between expose all or block all. Results implied that participants considered the system as easy to understand and favored manual authentication. The work of Hayashi et al[21] explored both usability of an all-or-nothing mechanism and new access control. In their study, 20 people who owned a tablet as well as a smartphone were interviewed. Results showed that an all-or-nothing device access control poorly met user' expectations, and the new control method was much more appealing to the them. The limitation of this study is that participants were asked hypothetical questions, which only partly reflect their real opinions and decisions.

One of different alternative solutions to let users take over control 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. In the past, many studies have focused on providing users' with tools to deliver privacy control to users. Some studies tried to propose and build protection tools like "Apex"[22] and "ProtectMyPrivacy"[23] to help users 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 imposes 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 focuses on identifying malicious behavior and monitoring data leakage of apps,[24,25] but without investigating usability of these tools and users' perception and reaction when reading the accompanying complex information.

2.3 | Comparison of privacy features on smartphone OSs

We analyze, compare, and discuss features on smartphone OSs. We searched and listed four smartphone OSs, including Android OS, iOS, Window Phone OS (WP), and BlackBerry OS, which have been embedded with features the same as or similar to Find My Device (FMD), Backup (BP), Location Blurring (LB), and Guest Mode (GM), as shown in Table 1. All four OSs have been equipped with features of Find Device and Backup. iOS and Android OS are equipped with Find My iPhone and Android Device Manager, respectively, including both app and online services. Similarly, Windows Phone OS offers Find My Phone in Settings and online service. BlackBerry OS 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. Since it has the potential risk of leaking stored data, many works have endeavored to provide useful mechanism.[26] From the perspective of users, they 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,[16] 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." In Table 2, we also consider Firefox OS, mainly comparing control and user effort levels on OSs, based on the taxonomy of Android permission models.[27] The analysis of location control methods reveals that Android, Windows Phone, and BlackBerry support blocking/unblocking location for all apps generally, while iOS and Firefox OS offer a more flexible control over each app. We categorize the degree of control the OS

TABLE 1 Privacy features available on OSs

Features	OSs
Find My Device	Android OS, iOS, WP OS, Blackberry OS, Firefox OS
Backup	Android OS, iOS, WP OS, Blackberry OS, Firefox OS
Location Blurring	Firefox OS
Guest Mode	Android OS, iOS, WP OS, Blackberry OS, Firefox OS

TABLE 2 Comparison of location protection on OSs

OSs	Control method	Feature	Control level	Required effort
Android	general	Block/ Unblock location	low	low
iOS	per app	Block/ Unblock location	medium	medium
WP	general	Block/ Unblock location	low	low
BlackBerry	per app	Block/ Unblock location	low	low
FirefoxOS	per app	Location Blurring	high	high

TABLE 3 Overview of guest mode feature on OSs

OSs	Initial release date	Feature
Android	November 2014	Multiuser account
iOS	Improved in 2014	1. Guided Access 2. Restrictions
Windows Phone	October 2012	Kids Corner
BlackBerry	August 2012	Parental Controls

allows users for different apps into three abstract levels, ie, low, medium, and high. Although iOS supports users to grant or refuse location requests from individual apps, users cannot obtain practical information from location-based services without revealing precise location information. On the one hand, such binary control measures are easy to use; on the other hand, unnecessarily exact information may be provided to certain apps, as discussed above. In turn, when a fine-grained user control is possible, more effort is required for making appropriate selections. In this work, we explore the balance between the amount of control and the effort for making adjustments.

Smartphone OSs started to attach more importance to the feature of "Guest Mode" since 2014 (see Table 3). 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. Besides, iOS has a Restriction feature that limits specific functions and apps. In the early stage of this feature, it does not apply to third-party apps nor does it provide access control for data. However, with the further evolution of iOS, the Restriction feature has included more flexible control and can be used not only for kids but also for other guests. Similarly, Windows Phone is equipped with *Kids Corner*, which regards the kid as guest and limits the usage of the phone to protect the kid. BlackBerry also provides a parental control app, similar to other OSs. Since kid usage is a specific and important guest user mode, we include the OSs, which only support parental controls. Moreover, since specific adaptations on what can be used are possible, this mode can be applied to other user groups than kids as well. Besides the kid mode, BlackBerry supports context-sensitive user data protection and respective management of data for users. Users could use one smartphone to work with a professional context and also use it for private purposes without mixing the two sets of data. This is another type of improved access control for privacy settings but with a different purpose.

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.

3 | PRIVACY FEATURES TO BE CONSIDERED

In this section, we briefly describe the privacy features that we are studying, including *Find My Device*, *Backup*, *Location Blurring*, and *Guest Mode*.

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 this feature, the user is able to pick the storage location, be it a default Mozilla server, some popular storage providers, or the personal computer, with respect to Location Blurring (see Figure 1A) by which 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 (see Figure 1B) can be divided into three groups, ie, applications, data, and resources. This feature consists of two parts, ie, 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. Upon entering the Guest Mode, the data stored in each of defined elements is substituted with an empty list, just as if

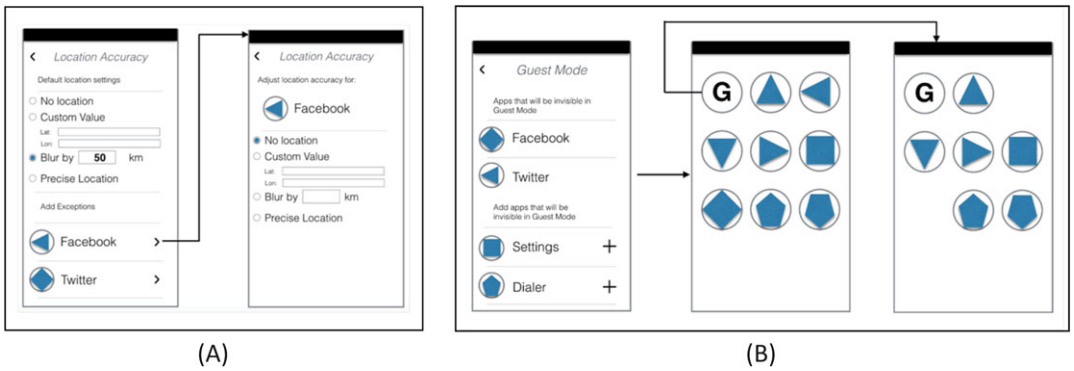

FIGURE 1 Location Blurring (A) and Guest Mode (B)

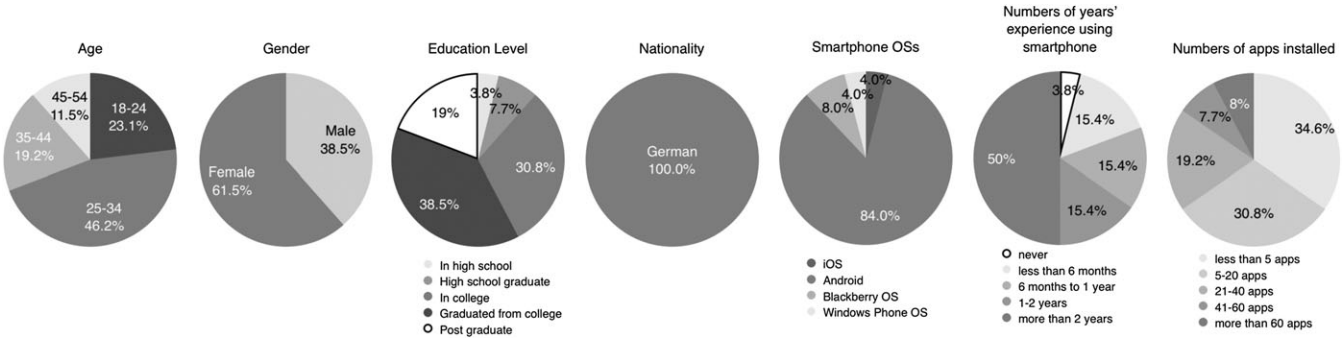

FIGURE 2 The demography of participants in the lab study

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, and browser history. Lastly, there is a possibility of limiting the access to the resources, like WiFi, cellular data, etc.

4 | USER STUDY

To obtain a profound understanding of peoples' mental models on privacy features, we organized a structured usability lab study of 26 users and a survey of 223 participants. We present the survey and its results after the lab study.

4.1 | Lab study on user control of privacy settings

In the lab study, we explored main research questions as follows.

- How do people perceive privacy? What is the link between the privacy settings and their mental model?
- What is the importance of privacy as a decision-making factor in different contexts related to personal data?
- How do users interact with personalized settings and how do they adapt to the world of full control over the ecosystem?

4.1.1 | Participants and procedure overview

We recruited participants from Prometei, a database for recruiting evaluation subjects to enhance the human-computer interaction, and offered 15 euro for participation. Participants did not need to own a smartphone. Some of them had feature phone but experienced using a smartphone when they borrowed a device from acquaintances.

The demography of participants in this lab study is as shown in Figure 2, including the age, gender, education level, nationality, smartphone Oss, and the experience in using smartphone. In total, we had 38% male and 62% female participants. Their ages were distributed between 17 and 55, with the breakdown to 23.1% in the group 18 to 24, 46.2% were 23 to 34 years old, 19.2% between 35 to 44, and 11.5% belonged to the category 45 to 54. Most of the participants (38.5%) graduated, and 30.8% were still in college. 19.2% obtained a higher education level like a master degree. The rest finished their education on high school level or the level before high school. Thus, there was a bias toward higher education. However, we managed to get a group of well distributed occupations, including students, graphic designers, secretaries, clerks, lawyer assistants, project managers, etc. Based on the above demographics, we believe that the opinions expressed and behaviors performed by participants are representative across age groups and genders of the smartphone users and the feature phone users in a smartphone environment.

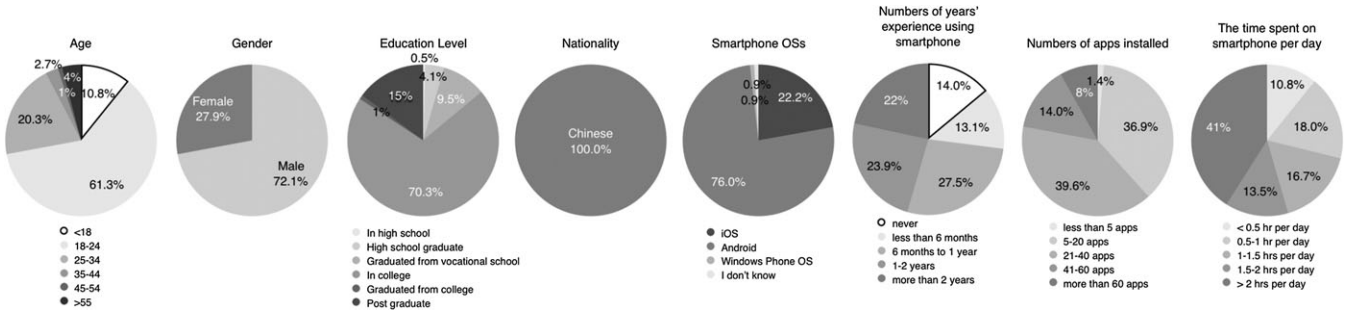

FIGURE 3 The demography of participants in the survey

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 features, 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 toward privacy and their choices in the privacy settings.

4.2 | Survey study on current usage of privacy features

In this survey, we recruited participants who were required to be the smartphone owner, using Wenjuan website to collect their answers, which is the one of the influential online crowdsourcing platform in China. We had 223 participants and obtained 222 pieces of responses. We present an overview of participants in Figure 3. Besides basic information, the numbers of years' experience using smartphone, numbers of apps installed, and the time spent on smartphone per day are also obtained. Participants were composed of 72.1% males and 27.9% females. Their ages were distributed and covered all age groups while 61.3% were between ages 18 to 24. There was a bias toward higher education levels and 78.9% were under a higher education. The occupations were variously distributed and participants were consisted of students, IT engineer, financier, project managers, freelancer, lawyer, designer, policeman, etc. 75.7% of participants were using Android OS, and the rest of them using iOS (22.1%), Blackberry OS (0.0%), Windows Phone OS (1.4%), Firefox (0.0%), and others (0.0%).

5 | RESULTS

In this section, we present the results of our user study, which are from the lab study (Sections 5.1 to 5.5) and the survey (Section 5.6).

5.1 | Privacy settings and weight of privacy

We take the definition of mental model presented in the works of Sharp et al[28] and Norman.[29] It is an explanation of users' thought process and their perception of how things work in real world. Although it is hard to meet such criteria, as it dynamically changes, it is important to aim at a design that would try satisfying it in order to make the system more intuitive and improve the adaptation rate. In order to determine the best fit, we asked the participants to decide how far do the settings influence privacy, rate wireframes with different positioning of the settings, and express their comments.

First, to gain a better understanding of how strongly do participants connect the features to privacy, we asked them to express their opinions on a five-point Likert scale, where anchor points are 1 - Strongly disagree and 5 - Strongly agree. They have judged each feature differently, ie, Find My Device and Backup were conceded to privacy at a lower level while Location Blurring and Guest Mode were at a high level (FMD: Mdn = 4; BP: Mdn = 2; LB: Mdn = 5; GM: Mdn = 5).

Next, in order to verify the users' mental model around the arrangement of privacy features, we designed and proposed seven wireframes. The designs were not final product proposals but rather prototypes that presented how our tool could be placed around the smartphone.

- Option 1: All 5 features are on the Home Screen, have distinct icons like other apps, and distribute and appear only once on the phone.
- Option 2: All 5 features are under the Settings like other functions and distribute and appear only once on the phone.
- Option 3: Some features are under the Settings and some of them on the Home Screen and distribute and appear once.
- Option 4: All 5 features are grouped as Privacy settings on the Home Screen and appear once.
- Option 5: All 5 features are under the Settings but are grouped in the category of Privacy and Security, appearing once.
- Option 6: Some features are under the Settings and all of them on the Home Screen as a group. The features appear twice on the phone (see Figure 4).
- Option 7: All of features are under the Settings as a group, and some on the Home Screen. The features appear twice.

FIGURE 4 Wireframe option 6 of privacy setting on smartphone

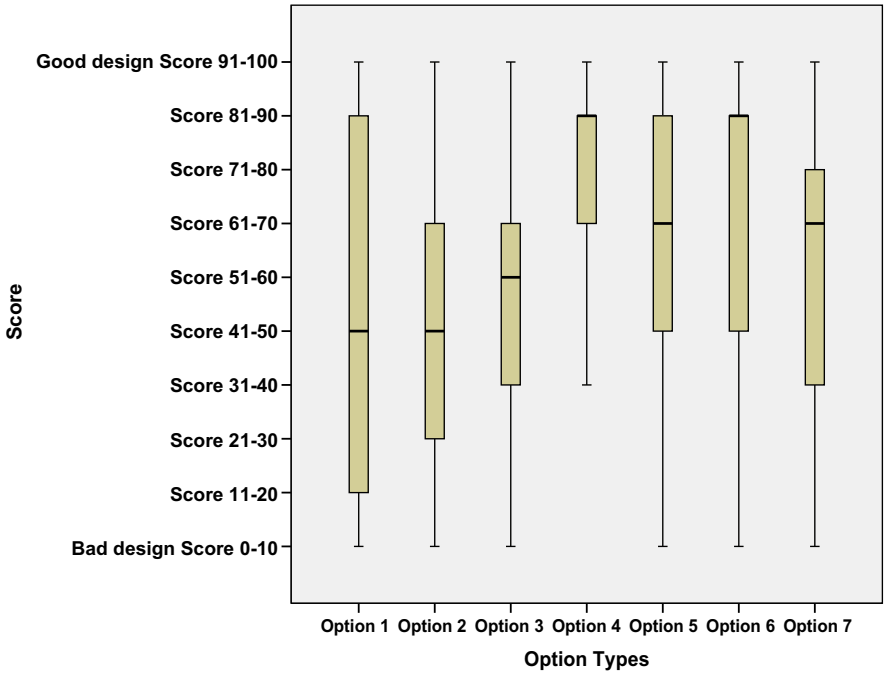

FIGURE 5 Scores of options given by participants

We adopted and defined references "Good Design" and "Bad Design" to help users make decisions. "Good Design" refers to a situation where the feature is easy to locate and it is understandable why it is placed there. As expected, a "Bad Design" refers to the opposite case. In such setting, it is hard to navigate around the phone, and the reasoning behind such decision is not clear. Based on these references, we asked participants to rate options and select the favorite one. Results showed that 34.6% of participants chose option 6 as their preferred arragement, and 23.1% of them selected option 4 as the second best version. As illustrated in Figure 5, users chose options 4, 5, 6, and 7 much more frequently than other ones. We also would like to know if participants would be confused by the features appearing in more than one place. Using the 7 point scale of semantic differential technique,[30] with paring of "Not confused/Confused," we found that 73% participants were not confused if privacy features appeared twice, with the median score at 6.

5.2 | Find my device

We started to discuss the privacy features of Find My Device, which has been embedded in most of the OSs. We asked participants to set up the Find My Device, and then recorded the values of settings. With regard to the way that users preferred to control the phone remotely, 23.1% chose to use SMS control only and 38.5% selected to use server control only. 34.6% selected to use both server and SMS control. Among these people who preferred to use SMS control (57.7%), 60.0% participants reported they would use all commands including start tracking, stop tracking, remotely wipe, and make a sound. 40.0% of them predefined part of commands for the further use. Almost all of them selected to use the command of making a sound. Additionally, we asked the users whether they would like their location to be remotely reported and where it should be sent. The possibilities

provided were phone number from which the request came, predefined number, and a predefined email address. Overall, 88.4% participants said they would like to use this service. Among them, 65.4% chose the email reporting, while 57.4% preferred the SMS method.

We asked participants to give scores to the factors that influenced their decisions on the control methods - why do they choose emails or text messages to control the phone remotely. The four main reasons that 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 6A). 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 (giving the scores of 5, 6 and 7) impacting their way of controlling smartphone remotely. They gave high scores to safety (Mdn = 7, as many as 84.7% of participants gave scores above or equal to 5), ease of accessibility (Mdn=7, 92.4% gave scores above or equal to 5) and ease of navigation (Mdn = 6, 57.5% gave scores above or equal to 5). About 61.5% did not consider the cost (like SMS costs) as a decision-making factor (Mdn = 2).

5.3 | Backup

We wanted to explore how much people care about the safety of their data - will they backup their smartphones and if they choose a full or partial copy. It indicated that only 38.5% decided to make a one to one copy of their data, while 61.5% chose a partial option. We found that there are differences between high-level private data like contacts, photos, and low-level private information like applications and music (see Figure 7). Participants, who did not backup applications and music, said that they would like to copy sensitive or important personal data, while it is possible to download apps and music again. With respect to frequency of backup, 42.3% participants chose to run it once a week, and 38.5% preferred to do it once a day. Only 15.4% and 3.8% users wanted to backup their smartphone every hour or every three hours, respectively.

The next question was where would the users store their backup. We provided five options, including personal computer, external SD card, Dropbox, Mozilla Cloud, and Deutsch Telekom Cloud (DT cloud). Overall, results showed that 52.8% of participants selected more than one place to store data, while 47.2% participants chose only a single location. Surprisingly, only 34.6% chose to store their private information at a cloud service, like Mozilla, Dropbox or DT Cloud. However, as high as 30.8% participants chose to use Dropbox, which reflects that they did not realize the potential

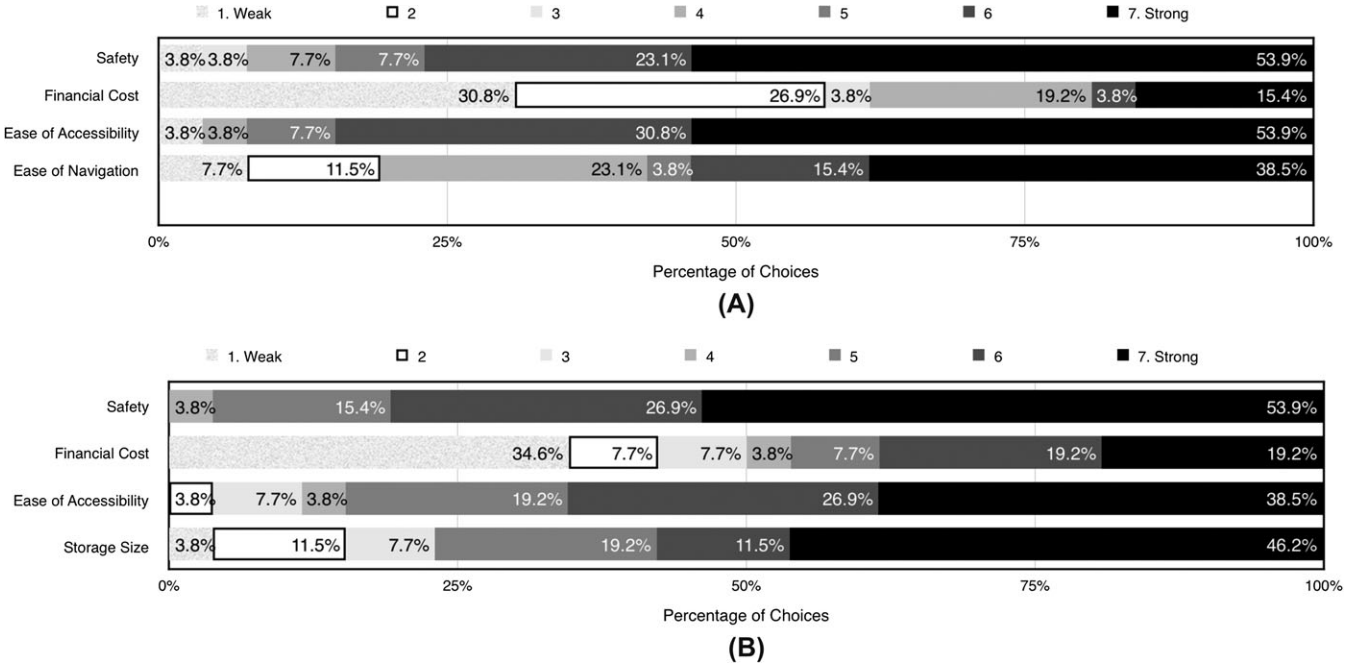

FIGURE 6 The percentage of participants selecting. (A) the factors that influenced their decisions on the control methods in Find My Device. (B) the factors that influenced their decisions on the storage place in the Backup

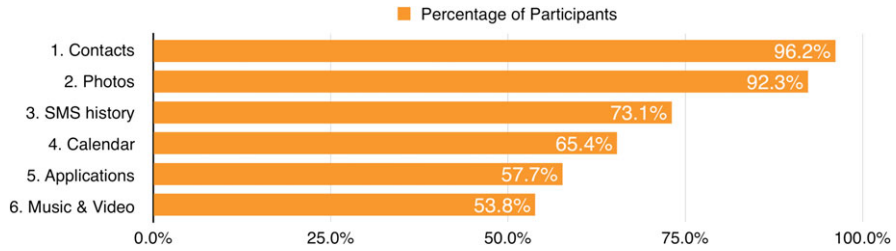

FIGURE 7 How participants selected to backup their data

risk of a free cloud service. One of the participants who selected Dropbox argued that he could access to his data everywhere and would not lose his information. 15.4% chose to use a personal computer as means of storage. To understand if people would be inclined to use an interface based manager to monitor all copies, we used Likert items based on a seven-point scale with anchor points of "1 - Strongly Disagree/7 - Strongly Agree". The median score of willingness is 6. Actually, as much as 76.9% of users were at least not against such a proposal; they chose 4 or more. Among these people, 85.0% said that they wanted to use such a manager on their smartphone.

The final question that we asked was the indication of how strongly each factor influences their decision with respect to storage place (see Figure 6B). We proposed four factors, ie, safety, financial cost, ease of accessibility (eg, cloud can be accessed anywhere at any time when connecting Internet, but PC cannot), and storage size. We employed a seven-scale semantic differential technique, as shown in Figure 6. All participants except one considered safety as having a strong impact (scores above 4, 96.2%). As illustrated in Figure 6B, they gave high scores to safety (Mdn = 7, 96.2% gave scores above or equal to 5), ease of accessibility (Mdn = 6, 84.6% gave scores above or equal to 5), and storage size (Mdn = 6, 76.9% gave scores above or equal to 5). About 46.1% said that the cost affected their decisions (Mdn = 3.5).

5.4 | Location blurring

A prior study by Tang et al[31] 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 (see Figure 8), which have been selected based on categories from preinstalled apps like browser, and from marketplace, including games, social networking, video, utility, fitness, etc. 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, and 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)."

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 an 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) are 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

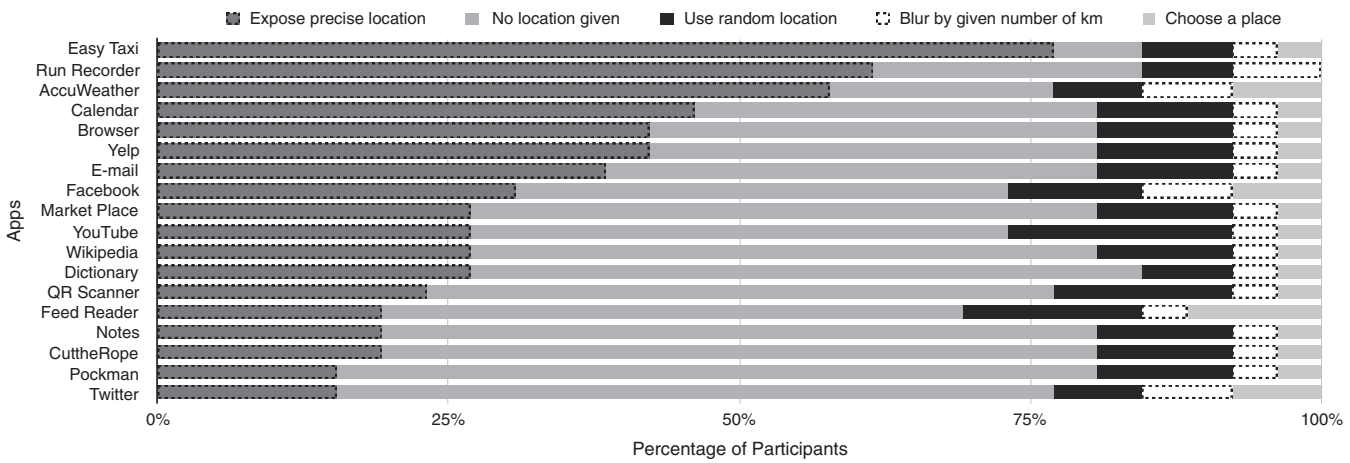

FIGURE 8 How participants used Location Blurring to protect location information

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).

5.5 | Guest mode

To know how users create profiles for different persons, we asked them to set up Guest Mode for different types of lenders respectively. We proposed actors based on relationships used in xShare,[8] however differentiated child (under 18 years old) from others. In total, we had nine types of lender including stranger, acquaintance, coworker or classmate, relative, parents, sibling, child, spouse, and friend. As shown in Figures 9 and 10, the x-axis represents percentage of participants, and the y-axis represents the resources, data, and apps that the participants to expose or hide for guests. From the perspective of guest roles based on trust levels, we observe that guests can be divided into three groups, ie, stranger, limited trust (acquaintance, coworker/classmate, and child), and higher trust (relative, parent, sibling, spouse, and friend). WiFi is the one resource that has been always made available to a guest.

In Figures 9B and 10, 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, ie, very limited trust (stranger, acquaintance, coworker/classmate, and child) and higher trust (relative, parent, sibling, spouse, and 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. In addition, calls made and SMSs

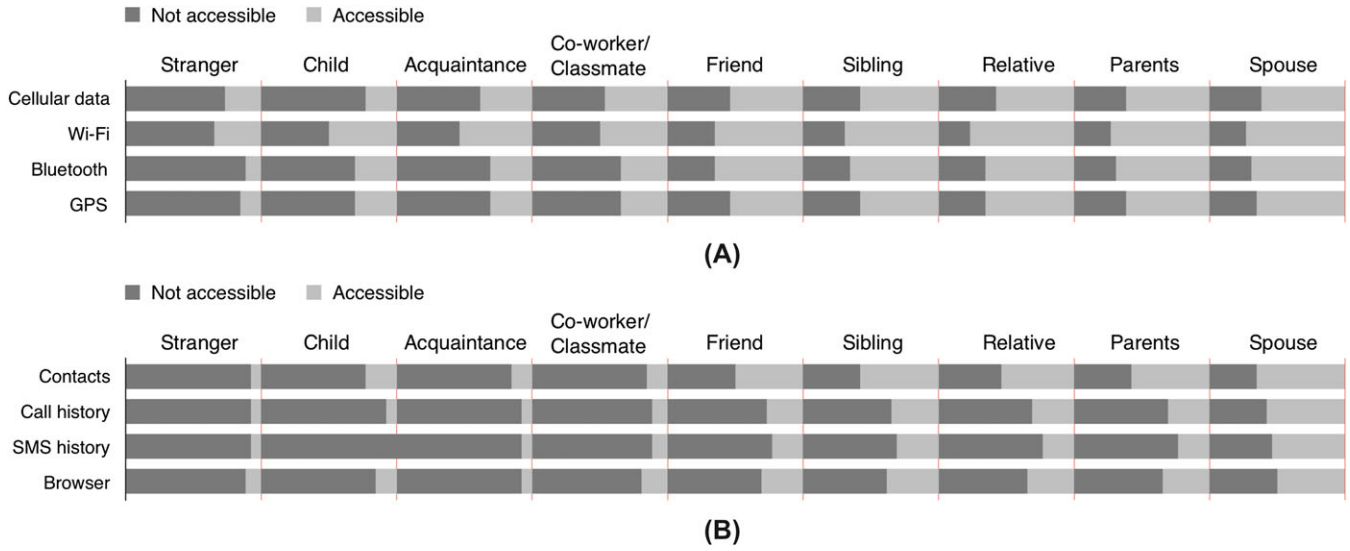

FIGURE 9 Percentage of responses on blocking/unblocking resources (A) and data (B) to nine actors

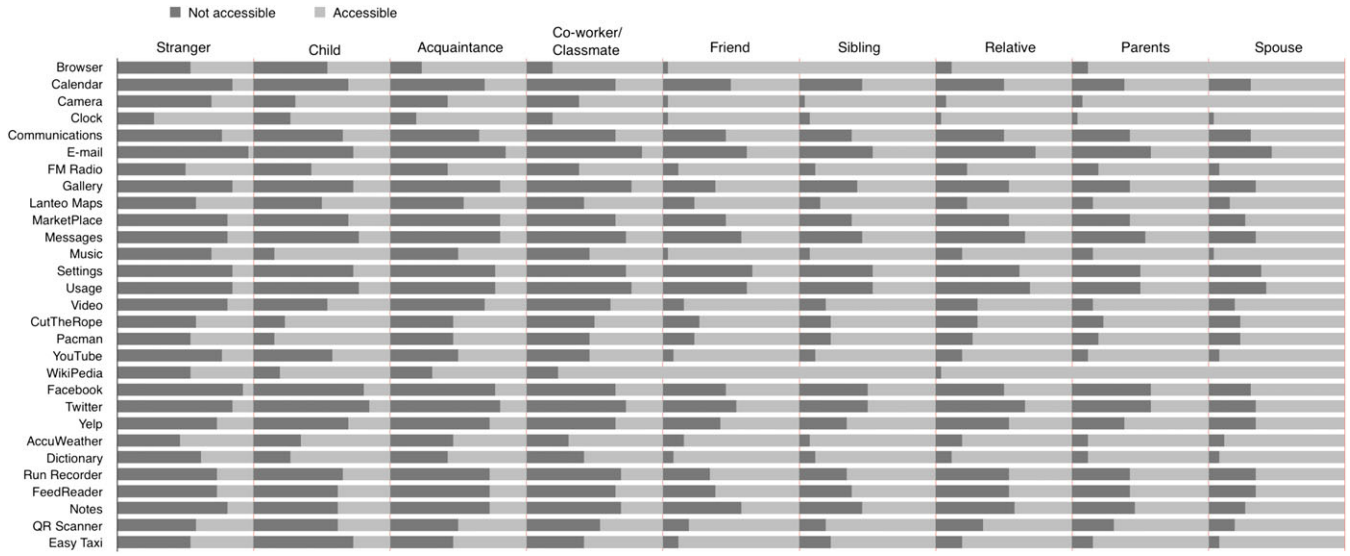

FIGURE 10 Percentage of responses on blocking/unblocking apps to nine actors

TABLE 4 Associations between age, gender, smartphone OS, income, education level, and whether participants use privacy and security settings

Associations	chi-square	p	phi
age-whether participants use privacy and security settings or not	33.589	.000**	.389
gender-use or not	.863	.353	.062
OS-use or not	4.840	.184	.148
income-use or not	19.057	.025*	.293
education level-use or not	26.283	.000**	.344

*Correlation is significant at the 0.05 level. **Correlation is significant at the 0.01 level.

sent were rarely exposed to them. It is obvious from Figure 9B that contacts, call history, SMS history, and browser contain sensitive and important personal information.

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, and 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.

5.6 | Current usage of privacy features

The results were obtained from the well-organized survey. We selected four main privacy features based on our previous research experience on Firefox OS,[32] including Find My Device (FMD), Backup (BP), Adjustable Location Accuracy (ALA, namely, Location Blurring), and Guest Mode (GM). Adjustable Location Accuracy feature is to protect geolocation privacy by adjusting accuracy of location, which has a counterpart like Fake Location (FL) on other OSs but beyond FL. Guest Mode feature personalizes the setting to block and hide some apps and resources like "Guest Mode" in PC, which has a counterpart like multiuser account on Android and restriction on iOS. We evaluated the usage rate of these four features on other OSs like iOS, Android, etc. Results showed that people were not aware of new features like Fake Location and Guest Mode and they used privacy features not at a high rate globally on their phones. The main reasons that participants did not use FMD and BP are either they did not know this feature (FMD: 38.6%, BP: 20.6%) or they knew this feature, but they did not know whether they needed it (FMD: 22.8%, BP: 35.3%). For Fake Location and Guest Mode, the main reason is that they did not know this feature (FL: 73.1%, GM: 71.9%).

In addition, we found that generally 90.1% of participants use privacy and security settings like screen lock, automatically lock, encrypt phone, verify apps, etc, on smartphone, while 9.9% not. Among the participants who said no, 65% expressed that they did not have important or sensitive personal data so they did not need privacy and security settings. Finally, participants used more privacy protection apps/services released from OSs than that of third party.

To know the factors that impact whether participants use privacy and security settings, we did the correlation test. The variables and their levels of measurement are age (ordinal), gender (categorical), education level (ordinal), income (ordinal), smartphone OS (categorical), and reaction on whether participants use privacy and security settings (categorical: Yes, No). Thus, we used Pearson's chi-square test to test associations between age, gender, smartphone OS, income, education level, and whether participants use privacy and security settings. There were no significant associations between gender and whether participants use privacy and security settings, as well as OS and use or not (see Table 4). We found whether participants used privacy and security settings were related to age, income, and education.

6 | DISCUSSIONS AND IMPLICATIONS FOR DESIGN

In this section, we discuss the main findings and limitations of this study and provide implications for design.

6.1 | Findings

How do people perceive and explain the linkage between their mental model and privacy features? The first conclusion is that users did not connect all of the features that we proposed to privacy. In particular, the storage of personal information has not been integrated with privacy protection in the mental models of most participants. However, in terms of placement, they still prefer having all five elements combined together in Privacy settings and placed on the Home Screen.

What is the relative importance of privacy as one of the decision-making factors in different contexts connected to personal data? The results showed that the participants are mostly concerned with the physical safety of their devices, being able to find it as soon as they noticed missing it and remotely control it. Similar is the motivation behind choosing the backup storage. 76.9% of users were not against using a manager interface on

their smartphone to navigate around the copies of their data. However, almost as high as 30.8% of participants would use Dropbox, which reflects that they did not realize the potential risk of a free cloud service.

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 be then given similar location 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.

What is users' current usage of privacy features? The main reasons that participants did not use Find My Device and Backup are either they did not know this feature or they knew this feature, but they did not know whether they needed it. For Fake Location and Guest Mode, the main reason is that they did not know this feature. There were no significant associations between gender and whether participants use privacy and security settings, as well as OS and use or not. However, we found whether participants use privacy and security settings were related to age, income, and education.

6.2 | Limitations

We paid a lot of attention to performing the study in the most reliable way and simulating using a phone in a real-life situation. However, there are some factors may have skewed our results like all controlled lab study. First and foremost, participants were not using their own devices. Mostly, they could be less motivated and engaged in setting up the phone. Although everyone were in the same situation, this might have also altered our results. A solution would be using automatic logging tools integrated in the system. In this way, all participants could install it on personal devices. In that case, we could perform a field study over a longer period of time. However, that would require a higher-level of technical support and prolonged time. Second, we did not dig deep the reasoning behind each decision. Privacy heavily depends on personal preferences; it is thus important to investigate personal opinions. This could be improved if we organize a semi-structured interview or focus group to interpret these reasons.

6.3 | Implications for design

Based on the findings presented above, we outline and discuss implications for the design to improve privacy control and awareness, including suggestions on settings, control, and interface.

6.3.1 | Settings beyond settings

With the increased requirements to be in better control over the phone, it is important to support users in the process, by choosing the right arrangement, naming, and helping in navigation around the privacy controls, within and outside the Settings app. Although smartphone OSs become increasingly more complex, commonly, most people explore the system hardly looking into the user manual. Thus, in order to satisfy users' expectations, it is essential to understand the linkage between their mental models and privacy features.

6.3.2 | Privacy as a decision-making factor

Our study showed a significant inconsistency in terms of privacy protection behaviors. On the one hand, users consider privacy and security important, maybe even crucial. On the other hand, they ignore it and give up personal data. We recommend providing tutorials and better education on privacy properties, even this is a lengthy process. Although raising awareness of some of the misunderstandings is hard, it is important to reinforce the concept of protecting personal information. We argue that privacy protection is one of the salient parts, but users did not realize the level of privacy drop that happened between feature phones and smart phones. One of possible solutions is to provide usable interface or notifications to draw attention to the importance of privacy in specific context on smartphone. Mobile phones are closer to users than any other medium and can convey information in a quick and effective way.

6.3.3 | Accommodating to personalized control in app ecosystem

Finally, to help users in adaptation to the app ecosystem and personalized control, we propose introduction of better sorting and categorizing methods to connect applications and resources that have similar privacy impact. Next, we believe it would be valuable to add recommendation engine based on the user's preferences. To provide a better support for secondary users, we suggest providing default profiles, the access control of creating new profiles, and reusing profiles for similar guests based on the outcomes of our research in Guest Mode. Results on user behaviors toward exposing resources, data, and apps could be used for default settings.

7 | CONCLUSIONS

This study was motivated due to the missing studies on users' reaction on personalized privacy settings. In this paper, we have presented our work on exploring users' attitudes and behaviors toward the privacy control beyond all-or-nothing settings. We conducted a fine-grained study of participants' mental models and expectations of privacy features, including a lab study and a survey study. From this user study, we found that (1) Participants connected privacy with proposed features at different levels. (2) They regarded the privacy as an important factor in the context of finding back smartphone and selecting storage places. (3) People were satisfied to use complex access control, and sorting methods; recommendation and establishing profiles could help them balance between full control and interactivity burden. (4) The principle reason that participants did not use privacy features was that they did not know these features.

In our future work, we are going to perform a field study over a longer period of time and explore the reasoning behind each decision of participants. More privacy features will be considered to be included.

ACKNOWLEDGMENTS

We would like to thank Dominik from Mozilla Foundation, with whom we have worked in collaboration in this research. This work was supported by Telekom Innovation Laboratories, and projects of the National Natural Science Foundation of China (No. 61702417 and No. 61703259), the Shaanxi Natural Science Foundation (No. 2017JM6097), and the opening Project of State Key Laboratory for Manufacturing Systems Engineering (No. sklms2016001).

ORCID

Yun Zhou http://orcid.org/0000-0002-2306-8986

REFERENCES

1. Stojmenovic I, Wen S, Huang X, Luan H. An overview of fog computing and its security issues. *Concurrency Computat Pract Exper*. 2016;28(10):2991-3005.
2. Zhou Y, Raake A, Xu Tao, Zhang X. *Users' Perceived Control, Trust and Expectation on Privacy Settings of Smartphone*. Cham, Switzerland: Springer International Publishing; 2017;427-441.
3. Smetters DK, Good N. How users use access control. In: Proceedings of the 5th Symposium on Usable Privacy and Security; 2009; Mountain View, CA.
4. Zhou Y, Piekarska M, Raake A, Xu T, Wu X, Dong B. Control yourself: on user control of privacy settings using personalization and privacy panel on smartphones. *Procedia Comput Sci*. 2017;109:100-107.
5. Chin E, Felt AP, Sekar V, Wagner D. Measuring user confidence in smartphone security and privacy. In: Proceedings of the 8th Symposium on Usable Privacy and Security; 2012; Washington, DC.
6. Felt AP, Egelman S, Wagner D. I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In: Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices; 2012; Raleigh, NC.
7. Shklovski I, Mainwaring SD, Skúladóttir HH, Borgthorsson H. Leakiness and creepiness in app space perceptions of privacy and mobile app use. In: 2014 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2014; Toronto, Canada.
8. Liu Y, Rahmati A, Jang H, et al. Design, realization, and evaluation of xshare for impromptu sharing of mobile phones. *IEEE Trans Mob Comput*. 2010;9(12):1682-1696.
9. Karlson AK, Brush AJ, Schechter S. Can I borrow your phone? understanding concerns when sharing mobile phones. In: 2009 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2009; Boston, MA.
10. Li J, Zhang Y, Chen X, Xiang Y. Secure attribute-based data sharing for resource-limited users in cloud computing. *Comput Secur*. 2018;72:1-12.
11. Hang A, Von Zezschwitz E, De Luca A, Hussmann H. Too much information! user attitudes towards smartphone sharing. In: Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design; 2012; Copenhagen, Denmark.
12. Matthews T, Liao K, Turner A, Berkovich M, Reeder R, Consolvo S. "She'll just grab any device that's closer": a study of everyday device and account sharing in households. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems; 2016; San Jose, CA.
13. Zhou Y, Xu T, Raake A, Cai Y. Access control is not enough: how owner and guest set limits to protect privacy when sharing smartphone. *HCI International 2016 - Posters' Extended Abstracts*. Cham, Switzerland: Springer; 2016:494-499.
14. Liu Y, Gummadi KP, Krishnamurthy B, Mislove A. Analyzing Facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference; 2011; Berlin, Germany.
15. Netter M, Riesner M, Weber M, Pernul G. *Privacy Settings in Online Social Networks - Preferences, Perception, and Reality*. New York, NY: IEEE; 2013;3219-3228.
16. Kshetri N. Privacy and security issues in cloud computing: the role of institutions and institutional evolution. *Telecommun Policy*. 2013;37(4-5):372-386.
17. GSMA. User Perspectives on Mobile Privacy. Futuresight. 2011. Technical report.
18. Felt AP, Ha E, Egelman S, Haney A, Chin E, Wagner D. Android permissions: user attention, comprehension, and behavior. In: Proceedings of the 8th Symposium on Usable Privacy and Security; 2012; Washington, DC.
19. Kelley PG, Cranor LF, Sadeh N. Privacy as part of the app decision-making process. In: 2013 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2013; Paris, France.
20. Seifert J, De Luca A, Conradi B, Hussmann H. *TreasurePhone: Context-Sensitive User Data Protection on Mobile Phones*. Berlin, Germany: Springer Berlin Heidelberg; 2010;130-137.

21. Hayashi E, Riva O, Strauss K, Brush AJB, Schechter S. Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. Paper presented at: 2011 Symposium on Usable Privacy and Security (SOUPS); 2012; Pittsburgh, PA.
22. Nauman M, Khan S, Zhang X. 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; 2010; Beijing, China.
23. Agarwal Y, Hall M. ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing. In: Proceedings of the 11th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '13); 2013; Taipei, Taiwan.
24. Zhou Y, Zhang X, Jiang X, Freeh VW. *Taming Information-Stealing Smartphone Applications (on Android)*. Berlin, Germany: Springer-Verlag; 2011;93-107.
25. Enck W, Gilbert P, Chun B-G, et al. *Taintdroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*. Berkeley, CA: USENIX Association; 2010;393-407.
26. Li P, Li J, Huang Z, Gao C-Z, Chen W-B, Chen K. Privacy-preserving outsourced classification in cloud computing. *Clust Comput*. 2017;1:1-10.
27. Au KWY, Zhou YF, Huang Z, Gill P, Lie D. Short paper: a look at smartphone permission models. In: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices; 2011; Chicago, IL.
28. Sharp H, Rogers Y, Preece J. *Interaction Design: Beyond Human-Computer Interaction*. Chichester, UK: Wiley; 2007.
29. Norman DA. *The design of everyday things*. New York, NY: Basic books; 2002.
30. Tullis T, Albert B. Chapter 6-Self-reported metrics. *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics*. Waltham, MA: Elsevier; 2008:123-166.
31. Tang K, Hong J, Siewiorek D. The implications of offering more disclosure choices for social location sharing. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2012; Austin, TX.
32. Piekarska M, Strohmeier D, Zhou Y, Raake A. Because we care: privacy dashboard on Firefox OS. 2015. Accessed September 18, 2015. arXiv preprint arXiv:1506.04105.

How to cite this article: Zhou Y, Qi L, Raake A, Xu T, Piekarska M, Zhang X. User attitudes and behaviors toward personalized control of privacy settings on smartphones. *Concurrency Computat Pract Exper*. 2018;e4884. https://doi.org/10.1002/cpe.4884