

# On the trade-off between privacy and utility in mobile services: A qualitative study

Yang Liu<sup>1,2</sup>[<https://orcid.org/0000-0003-2486-5765>] and  
Andrew Simpson<sup>3</sup>[<https://orcid.org/0000-0003-3597-2232>]

<sup>1</sup> Harbin Institute of Technology (Shenzhen), Shenzhen, China

<sup>2</sup> Peng Cheng Laboratory, Shenzhen, China

[liu.yang@hit.edu.cn](mailto:liu.yang@hit.edu.cn)

<sup>3</sup> Department of Computer Science

University of Oxford, Oxford, United Kingdom

[andrew.simpson@cs.ox.ac.uk](mailto:andrew.simpson@cs.ox.ac.uk)

**Abstract.** While the widespread use of mobile services offers a variety of benefits to mobile users, it also raises serious privacy concerns. We report the results of a user study that investigated the factors that influence the decision-making process pertaining to the trade-off between privacy and utility in mobile services. Through two focus groups, 16 individual interviews and a questionnaire survey involving 60 participants, the study identified awareness and knowledge of privacy risks, trust in service providers, desire for mobile services, and belief of cyber privacy as four factors that contribute to the perceived trade-off. The results also suggest that, with appropriate adoption, privacy-preserving tools can positively influence the privacy trade-off. In addition, our findings explore the cultural differences regarding privacy between participants from western countries (with the UK as the main representative) and China. In particular, the results suggest that participants from China are more likely to be comfortable with a government department protecting their individual privacy, while participants from western countries are more likely to wish to see such responsibility reside with some combination of individuals and non-governmental organisations.

**Keywords:** Privacy · Mobile services · Human aspects

## 1 Introduction

It is well understood that, almost every time people attempt to use mobile services, they are making a decision to exchange their privacy for benefits. For example, people often need to provide their location to obtain a real-time weather forecast or share their interests to acquire accurate recommendations for goods or activities. Indeed, the economic model behind most free mobile services is based on such trade-offs: when using mobile services provided by Facebook or Google, users do not directly pay the service providers money to download or use their mobile services; rather, the mobile platforms collect a vast amount of users' personal data by analysing users' in-app behaviour. The personal data is then used to sell highly targeted ads.

People's attitudes towards such privacy issues vary significantly. Some users would be prepared to abandon the benefits provided by mobile services to protect their personal data. According to a survey of 2,000 Americans conducted by the Pew Research Center [6], 54% of mobile users have decided to not install an app when they discovered how much personal information they would need to share in order to use it and 30% of mobile users have uninstalled an app after discovering it was collecting personal information that they did not wish to share. Some others would enjoy the benefits without considering the potential privacy risks. A field experiment [5] showed that about 93% of participants are willing to provide personal data about their date of birth and monthly income for a 1 Euro discount for purchasing DVDs.

Various privacy-preserving technologies, with examples including permission management tools [13, 10], app analysing tools [2, 26] and privacy-preserving frameworks in specific fields [27, 17], have been proposed to help people decrease their privacy risks when using mobile devices. While the theoretical advantages of such privacy-preserving technologies are clear, little adoption has been observed in practice [4].

Online users' privacy concerns may vary depending on the situation [25]. In terms of mobile services, factors such as perceived convenience [20], perceived financial cost [18], expected degree of information disclosure and potential privacy risks [12] all play important roles and lead people to varying decisions. However, many questions still remain unanswered in this context. Such questions include: what factors influence people's decision-making processes?; what are the benefits of, and barriers to, using privacy-preserving technologies in this context?; what direction might be followed to foster adoption of such technologies?; and do cultural differences play a role?

To start to address these questions, we conducted a qualitative study by combining the methods of focus group sessions (two groups with five participants each), individual interviews (16 participants), and a questionnaire survey (60 participants). The objectives of this study were: to investigate the human factors influencing decision-making pertaining to the trade-off between privacy and utility in mobile services; to explore the direction that might be followed to foster adoption of privacy-preserving technologies that could help mobile users to balance privacy and utility in more effective ways; and to study the impact of cultural differences regarding the protection of privacy.

The paper contributes to the debate surrounding mobile privacy issues and to research into the adoption of privacy-preserving technology. It does so by presenting a detailed description of human factors influencing mobile users' decision making, and by presenting theoretical and practical guidelines for developers who are responsible for designing privacy-aware mobile services and for researchers who are interested in designing privacy-preserving mobile tools.

## 2 Motivation and background

Compared to the huge benefits received by users, the cost of mobile services is, on the face of it, extremely cheap. However, users pay with their personal information instead of cash. According to AppBrain [1], by the end of 2017 only about 222,600 of the total 3.5 million apps on Google Play were paid apps, meaning that more than 3.3 million apps were free to download. In addition, only about 275,700 of these free apps offer

in-app purchases — most of the rest are totally free to use and rely on in-app ads. The free app business model results in the collecting of a vast amount of users' personal data, as these apps need individuals' data to make the in-app ads highly targeted.

The highly involved mobile services and the free app ecosystem regularly lead mobile users into situations requiring them to make decisions. Almost every time they attempt to use a mobile service, they are making a decision to exchange their privacy (in terms of their personal information (e.g. age, location, monthly income, etc.)) for benefits. The utility of a mobile service is the measure of the worth or value it provides. Attitudes towards the trade-off between privacy and utility vary significantly. The results of a survey conducted by Marketing Land [19] suggest that close to half (46%) of respondents indicated either a neutral or unconcerned reaction to being retargeted by retailers, while the rest have concerns about the potential privacy risks.

Individuals behave inconsistently: not only do different people's attitude vary, but the same user may choose different strategies to handle the trade-offs when using different mobile service as various factors might be involved in their decision-making process. For instance, when facing the trade-off between receiving the benefits of a mobile coupon and giving up personal information, factors such as perceived value and 'coupon proneness' could positively affect the user's acceptance of related apps, whereas perceived fees and perceived privacy risks might impact negatively [15].

The inconsistency between people's privacy attitudes and their final decisions makes for a complicated state of affairs. Deciding to use an app does not necessarily indicate a lack of concern about privacy. Users might take a number of steps such as clearing their browsing and searching history or turning off the location-tracking feature on their mobile devices to protect their personal information before enjoying mobile services. On the other hand, users who claim they have a serious concern about privacy risks might also share their personal information willingly for certain benefits. People's observed behaviour being inconsistent with their reported attitude to privacy is usually termed the *Privacy Paradox* [3].

Our aim is to understand how human factors can impact upon the decision-making process pertaining to the trade-off between privacy and utility in mobile services. We are also interested in understanding whether certain privacy-preserving technologies can positively influence such a trade-off. In addition, we want to explore the impact of cultural differences.

This research presented several challenges:

1. **Privacy paradox.** Despite the various levels of privacy awareness and knowledge of participants in this study, people's stated attitudes may be influenced by the so-called privacy paradox. As such, users' observed actions should also be used to infer the level of privacy concern [23].
2. **Cultural differences.** Privacy concerns and related approaches of protecting privacy vary between cultures [7]. The interview subjects of our study (26 participants in total) were drawn from diverse cultures and backgrounds (38% were British, 38% were Chinese, and 24% were participants from other countries).
3. **A complex array of factors.** People's decision-making can be affected by a complex array of factors. It is important to declare that the human factors we discuss

**Table 1.** Participants description

Group(N)	Type	Description
Cyber security doctoral students (5)	Focus Group	Cyber security doctoral students in a university in the UK, between 26–45
Non-technical (5)	Focus Group	Adults of various countries, various occupation, and various ages; two members between 26–35, three others between 36–45
Young British adults (8)	Individual Interview	Young British citizens, between 26–35
Young Chinese adults (8)	Individual Interview	Young Chinese citizens, between 26–35

in this study cannot fully explain the decision-making process. In addition, these factors and their importance to the participants are relatively subjective.

### 3 Methodology

We now introduce the qualitative approaches adopted in our study and present details of the scenarios and the design of questions.

#### 3.1 Study approaches and participants

This study was conducted in Oxford, UK, in February 2017. Two primary qualitative approaches were adopted: focus group interviews (10 participants) and individual interviews (16 participants). In addition, a questionnaire survey (60 participants) also provided auxiliary data.

Focus groups are useful for gathering detailed information about both personal and group feelings [14]. A broader range of information can also be collected from the interaction and discussion among the participants. By contrast, individual interviews are helpful for researchers to probe more deeply on each topic and get information from non-verbal responses [9].

Two groups based on participants' technology backgrounds were selected for the current study. Members of the first group were doctoral students in the field of system and software security. Instead of the strong knowledge of security technology, the second group was internationally diverse: the members are adults from five different countries with different occupational backgrounds. The focus groups were set up in such a way to ensure appropriate interaction within each group and to provide a clear contrast between different groups, enabling us to better discuss how awareness and knowledge of privacy risks might affect the decision-making process.

The participants of individual interviews were also categorised into two groups to investigate the similarities and differences between attitudes between young British citizens and young Chinese citizens. The interviews with Chinese residents were conducted via Skype in the language of Chinese. The individual interview groups were set up in such a way to collect comments from participants from different cultures.

The group size of each focus group session was 5 and the size of each individual interview category was 8. The total number of interview subjects was 26. All participants were asked to complete a questionnaire<sup>4</sup>, which was used to deduce participants' privacy attitudes, as a pre-survey before they attended the interview.

Participant recruitment was conducted by posting posters on Facebook and Wechat Moments (social networking), and by circulating advertisements through the mail lists of different departments, colleges, and clubs of Oxford University. All of the subjects were offered a £10 Amazon gift voucher for their time. The distribution of participants is shown in Table 1.

### 3.2 Scenarios and data collection

Wash *et al.* [29] argued that the result reflected by users' actual behaviours is more accurate than that collected by their self-reports when studying certain user decisions. To better measure participants' actual behaviours, a card-exchanging game was applied in the focus group sessions to start off the discussion.

Participants were asked to play the roles of "mobile users" and "service providers" in a two-round card-exchanging game. Five cards representing personal information (including gender, location and contacts list) were issued to "mobile users" and five cards representing mobile services (e.g. real-time weather forecast, recommendations of interested activities and a £5 Amazon voucher) were issued to "service providers". In the first round, "mobile users" were asked to select between zero and five information cards they can afford to disclose, then exchange them with the corresponding number of service cards decided by "service providers". In this round, "mobile users" were not able to figure out the service cards they could obtain before the trade was finally made. In the second round, "service providers" were asked to show all their service cards before performing the trade. Therefore, "mobile users" were able to choose the particular service cards, and then exchange them with self-selected information cards.

Compared to traditional approaches (e.g. interview or focus group), the card game has an advantage in collecting users' actual behaviours. In the first round, participants are blind to the exact services they might receive, whereas, in the second round, participants are able to exchange specific service with self-selected personal information. Participants' actual behaviours under different conditions are observed and recorded during the game. In addition, the card game served as an icebreaker and helped participants to build mental associations with privacy and utility exchange.

Apart from the card game, the same scenarios were applied in both the focus group sessions and the individual interview sessions to collect participants' comments. At the beginning of each session, five scenarios that mobile users typically encountered in their everyday lives were presented. The aim was to explore participants' experience with balancing privacy and utility related to mobile services. The scenarios were:

- **Scenario 1.** Experience of exposing personal information actively: imagine that you are posting stories or photos on Facebook or Instagram.

<sup>4</sup> Full survey text can be accessed here:

<https://yangliu.typeform.com/to/OEPM6f> (English Version)

<https://yang46.typeform.com/to/PR3oWD> (Chinese Version)

- **Scenario 2.** Experience of interacting with mobile system providers: imagine that you are downloading an app from the official Android or iOS app stores.
- **Scenario 3.** Experience of receiving targeted recommendation services: imagine that you are visiting an unfamiliar place and you receive recommendations for useful information such as tourist attractions, hotels and restaurants on your mobile device.
- **Scenario 4.** Experience related to financial activities: imagine that you are doing online shopping on your mobile device.
- **Scenario 5.** Experience related to personal events: imagine that you are managing calendar events on your mobile device.

For each scenario, participants were requested to think about and comment on the following topics.

1. *What type of personal information do you think is being collected in this scenario?* (To explore participants' understanding of privacy leakage.)
2. *Who do you think is collecting your personal information? Where do you think your personal information will end up?* (To explore participants' perceptions of the leakage path of their personal information.)
3. *How do you think they collect or deduce your information?* (To explore participants' knowledge of the different personal information-collecting technologies.)
4. *In what ways do you think your personal information will be used? Do you see any potential risks?* (To explore participants' understanding of privacy risks.)
5. *What utility do you think is obtained in this scenario? Do you think it is worth the cost?* (To explore participants' feelings of, and attitudes toward, the trade-off between privacy and utility.)

They were then presented with a brief introduction to the Privacy-Preserving Targeted Mobile Advertising (PPTMA) framework [17] as an example technology. The framework was applied to the five scenarios to show how privacy-preserving technologies could help mobile users to take control of their sensitive information. The example also introduced the possibility of taking advantage of mobile services without compromising users' privacy.

After showing the examples, participants were requested to think about and comment on the following topics.

1. *What do you see as the benefits of using such privacy-preserving technologies?*
2. *What do you see as the barriers to using such privacy-preserving technologies?*
3. *Do you think such privacy-preserving technologies could influence your decision-making process with regards to making trade-offs between privacy and utility in mobile services?*
4. *Who do you think should be responsible for certifying that such privacy-preserving technologies do what they say?*

## 4 Results

The initial results indicate that the focus group members, individual interview members and questionnaire survey participants demonstrated a degree of consistency with

regards to their mobile service use. For example, about 80% of them spend more than 60 minutes on mobile services per day, with more than half of the total participants spending more than 120 minutes. The devices are mostly used for services such as social networking (90%), searching for information (88%), creating and checking emails (63%), and online shopping (53%). Furthermore, most of the participants had some experience in making decisions involving the trade-off between privacy and utility in mobile services.

#### 4.1 Factors contributing to the trade-off

**Awareness and knowledge of privacy risks** It is clear that the awareness and knowledge of privacy leakage is an important factor that strongly influences people's decision-making processes. The differences with regards to this factor between the groups was greater than expected. The findings suggest that the influences vary significantly due to the participants' various backgrounds.

Pöttsch [22] argued that privacy awareness enables people to make informed decisions about the disclosure of data. Our findings suggests that people with limited awareness and knowledge of privacy leakage are more likely to exchange their personal information for mobile services:

"If I know my privacy is compromised I would not make the trade-off. The key problem is that in many cases I didn't realise my personal information is being collected." (I2P6, Chinese, Female, Individual interview, Semi-skilled worker)

"I personally feel safe. Maybe because that I don't consider myself that important or special. I can't see why they want my information. So if Google requires my location details to provide services I'll give it without thinking about the trade-off" (G2P3, Finnish, Female, Focus group, House person)

On the other hand, many interviewees stated that they refused to make such trade-offs when sensitive information is required for exchanging services.

"Yes, I have refused to install apps that ask for very specific information. I tried to find substitutes in that case." (G2P1, British, Female, Focus group, Professional and managerial occupation)

"I didn't pay for using the apps so I understand they need my information to make money by some means. But for most apps, I would only use them if they promise that the data would only be used in aggregate form." (G1P4, American, Male, Focus group, Cyber security doctoral student)

The findings suggests that limited awareness and knowledge of privacy leakage could positively affect the user's acceptance of mobile services with risks of disclosing personal information. It is noteworthy that some interviewees acknowledged that they normally consider themselves to have serious privacy concerns in a pre-survey; however, in the subsequent card-exchanging game (personal information cards versus

**Table 2.** Auxiliary data: Awareness and knowledge of privacy leakage

*Questionnaire: To the best of your knowledge, which of the following information is technically possible to be collected/deduced by an app provider when you use an app? (Multiple choices)*

Item	China (43 participants)	Western Countries (17)	Frequency in total (60)
Your geographical location	38	16	54
Your phone number	29	15	44
Your contacts	26	12	38
Time of usage	20	17	37
Your email address	23	13	36
Your network operator	20	13	33
The list of apps installed on your phone	17	14	31
⋮	⋮	⋮	⋮
The retail price of your phone	4	7	11

mobile services cards), they unconsciously ignored the privacy risks and decided to make the trade-offs.

In addition, our findings show that, while most participants could identify the risks of privacy leakage about the information with a high exposure rate from public media (e.g. geographical location, phone number and contacts), certain personal information that seems difficult to collect (but, in fact, is not) is rarely considered by the users. Take “*the retail price of your mobile*” in Table 2 as an example: it is straightforward to obtain the information of the phone model. The phone model then leads to a precise retail price, which can then be used to deduce the spending power of the phone owner. Overall, participants showed relatively low awareness of such privacy leakage.

**Trust in service providers** Earp and Baumer [8] found that, if a site or a company is well-known, consumers would be more likely to disclose information to it. Similar comments received in our study suggests that trusting the reputation of a company would weaken users’ awareness of privacy risks from such a company and positively impact the adoption of the trade-off. The following representative comment indicates how *trust* can affect users’ privacy awareness and subsequently influences decision-making:

“I feel safe to use some mobile services because the companies like Google or Facebook are famous and so many people are using their services. Furthermore, the government can help to monitor them.” (I2P4, Chinese, Female, Individual interview, House person)

However, the extent that *trust* affects *privacy awareness* may vary according to users’ knowledge of privacy risks. Although a good reputation is viewed positively by participants with more privacy knowledge, such participants show stronger concerns under the same situation:

“I think I’m more scared of potential recruiters or potential employers looking at my profile on Facebook and use it to take advantage of me. So I never post



anything public. . . . We also know no matter I post it in public or private Facebook is going to get the information. I believe in Facebook as a company, but what about their employees. We all know stories like software engineer may hack into company's servers to steal others' personal information, which happened in Google previously. In addition, company like Facebook may share our profile with countless cooperative advertisers. Can we trust these advertisers as well? All these factors make me feel hesitate to use their services." (G1P5, Chinese, Male, Focus group, Cyber security doctoral student)

**Desire for mobile services** As already discussed, *awareness and knowledge of privacy risks* clearly influences the decision-making process. We predicted that, in general, a user with a relatively weak awareness of privacy risks is more likely to 'make the deal'. However, our findings suggest that a strong desire for specific mobile services may also enable users with strong knowledge of privacy leakage to bear the risks. For example, a statement made by a participant shows the ineluctability of using mobile service such as Facebook:

"I rarely post pictures or comments to Facebook and I'm careful with what I post and where from. However, as a small business, (to advertise my business) I have no choice about being on Facebook. If I didn't have to be I would avoid it." (I1P8, British, Female, Individual interview, Professional and managerial occupation)

Another statement made by a cyber security doctoral student with relatively strong knowledge of privacy risks also indicates how the *desire for mobile services* may work in this context.

"It's such pain to type in my address or my credit card details every time to shopping online. So I use Amazon app all the time. Because it already got my credit card details, already got my post address. If my friend recommends me a book I can buy it with one click and get it by tomorrow. I know Amazon is collecting my information, that's fine. I chose to have a business relationship with them. I'm happy that they have my address, my credit card details, my purchasing habits. Because I got good recommendation and also get cheaper items from them. I feel like they have more duty not to sell my information because they already got money from me." (G1P2, British, Male, Focus group, Cyber security doctoral student)

These statements suggest that, in some situations, the strong desire for mobile services may overcome the awareness of privacy risks and encourage users to disclose their information. For example, there is no substitute for the Facebook app, and the Amazon app may provide significant benefits — such as useful recommendations. The auxiliary data of Table 3 shows some factors that might encourage users to give personal information to an app.

**Table 3.** Auxiliary data: Impact of trade-off situations*Questionnaire: What might encourage you to give the information to an app? (Multiple choices)*

Item	China (43 participants)	Western Countries (17)	Frequency in total (60)
In exchange for access to the main functions of the app.	30	15	45
The app provides a statement regarding how the information is going to be used.	18	11	29
If there is no substitute for the app.	16	7	23
In exchange for a useful recommendation.	10	7	17
If the data would only be used in aggregate form.	5	11	16
In exchange for valued-added service.	10	3	13
In exchange for a small discount or coupon.	3	3	6

**Beliefs of cyber privacy** In addition to the particular situations introduced in Table 3, there is another encouraging factor that can be easily noticed: the common belief that cyber privacy does not exist or that “I’ve got nothing to hide”.

Phelan *et al.* [21] found that the belief that nothing is private online is often used by people as a reference frame to assess marginal risk in the context of privacy concerns related to online data collection. A significant number of participants made similar statements in our study.

“The services is worth the cost. Because, in fact, there is no so-called ‘privacy’ in the cyber world nowadays. We’re going to give out our privacy anyway, why not exchange it for some benefits?” (I2P1, Chinese, Male, Individual interview, Professional and managerial occupation)

“Our personal information is not only exposed by mobile. From this aspect, we don’t need to feel so sensitive. We are surrounding by internet, who can escape?” (I2P7, Chinese, Female, Individual interview, Semi-skilled worker)

“There are many ways to use our information. Maybe to improve the service to make you use it more or maybe they just want to sell it or use with advertisers. If we think too much we’ll have no app to use, because every app is doing this.” (I1P6, British, Male, Individual interview, Student)

#### 4.2 Desired adoption of, and trust in, the privacy-preserving technologies

Various types of privacy-preserving technologies have been proposed to help users handle the privacy and utility dilemma [13, 17, 26]. While the theoretical advantages of such tools are clear, little adoption has been observed in practice [4]. Some researchers have started to explore the direction that might be followed to foster adoption of privacy-preserving technologies [24]. Others (e.g. [16]) have provided foundations for future research on designing incentive schemes for privacy-sensitive users by proposing models to capture the interactions between businesses and consumers in the context of targeted advertising. In this study, we discuss our participants’ attitudes with regards to importing privacy-preserving technologies in this context.

Perhaps unsurprisingly, participants' responses suggest that they were in favour of privacy-preserving technologies that can provide utility for users to manage their personal information in mobile devices and can help users to increase their awareness when using mobile services. Such technologies have the potential to decrease users' privacy concern and establish a win-win situation for both users and mobile service providers.

"Yes, if I thought any technology could give me better service as a result of more fine-grained information I'd probably agree that such technology would influence my decision making process." (G2P4, Korean, Female, Focus group, white collar worker)

"Such technologies would make me more likely to download an app if coarse-grained data was collected only." (I1P4, British, Female, Individual interview, Student)

In addition, the same participants' different behaviours observed during the two-round card-exchanging game also echo the adoption of personal information management tools. Compared to the first round of the game, participants suggested that, in the second round — when they could clearly figure out what services they might obtain and when they were able to decide which part of their personal information should be submitted to the service providers — a better decision could be made.

While the necessity for privacy-preserving technologies is clear, participants expressed their concerns about the potential trouble caused by adopting such technologies. For example, some participants worried about the costs of learning how to use such tools. Some provided comments pertaining to their previous experience of receiving disturbing notifications caused by uninterrupted reminders from such tools.

"It's useful. But I think it's difficult for my parents to learn how to use it. They are not good at IT stuff." (I2P6, Chinese, Female, Individual interview, Semi-skilled worker)

"I get a bit annoyed once you use some apps and then you start to get notifications (from the privacy-preserving tools) reminding you to protect your data." (G2P5, Australian, Male, Focus group, white collar worker)

Participants also provided comments on basic requirements for decreasing such barriers, including configurability, easy deployment, privacy by default, and automatic activation. In addition to these requirements, there is a major concern about trust in such tools. Many people are still confused about the monitor in this context: who is responsible for certifying that such technologies do what they say? What if a privacy-preserving technology provider steals users' information under the guise of protecting it?

"It's tricky with electronic stuff. What's that to do with my data? ... If you have that stamp, then we know you follow the rules. That might be easier. But whose job is it (to give the stamp)?" (G2P2, Chinese, Female, Focus group, House person)

**Table 4.** Auxiliary data: Trust in the privacy-preserving technologies

*Questionnaire: Who do you think is responsible to certify such technologies do what they say?  
(multiple choices)*

Item	China (43 participants)	Western Countries (17)	Frequency in total (60)
Government department	22	4	26
Don't know	15	9	26
Organisations	3	5	8
Famous companies	3	1	4
Others	0	1	1

A noteworthy percentage (43%) of the participants cannot determine a suitable entity to play this supervisory role. Most of the remainder would be prepared to see an appropriate government department take the role:

“Government should publish related policies, and companies with high reputation should help to implement the policies and monitor related technologies.”  
(I2P5, Chinese, Female, Individual interview, Semi-skilled worker)

“Maybe the government but can they be trusted? I hope that third party standards exist but I’m not sure if they do and how or who could regulate them.”  
(G2P1, British, Female, Focus group, Professional and managerial occupation)

“To some extent the person downloading the app is responsible for checking what data will be taken from them, because when he accesses the (Android) app store, the app to be downloaded has already told the him what permission it needs and what information it will collect.” (I1P4, British, Female, Individual interview, Student)

Responses on this topic tended to differ between participants from different cultures, which we will explore further in the next subsection.

### 4.3 Privacy concerns across cultures

Kayes *et al.* [11] argue that users’ privacy concerns vary between cultures. Specifically, users from individualistic countries<sup>5</sup> tend to give more weight to privacy protection when compared with those from collectivistic countries<sup>6</sup>. Our study explored the influences of cultural differences regarding the protection of privacy.

The first interesting result emerged when we review the responses associated with “Trust in privacy-preserving technologies”. While more than half of Chinese participants (22 out of 43) stated that a government department should play a role in monitoring technology providers, the corresponding figure for participants from western countries was about 24% (4 out of 17). From a different aspect, our findings suggest

<sup>5</sup> Individualistic countries emphasis on prioritization of self over the group.

<sup>6</sup> Collectivistic countries emphasis on prioritization of the group over self.

that users from collectivistic countries are more likely to be comfortable with a government department protecting their individual privacy, while users from individualistic countries are more likely to see the responsibility reside with some combination of individuals and non-governmental organisations. Representative comments from each group are as follows:

“I go for the government. Because companies and organisations may take advantage of the monitor position for their own benefits. . . . (when asked about the possibility of government surveillance) Maybe, but it’s better to put my information in the hands of the government rather than in those of some companies.” (I2P2, Chinese, Female, Individual interview, White collar worker)

“I rely on information from groups such as ORG (Open Rights Group, a UK-based organisation that works to protect the rights to privacy and free speech online) at the moment, but all options such as government, organisations or famous companies are problematic.” (I1P8, British, Female, Individual interview, Professional and managerial occupation)

We also saw some similarities between participants from different cultures. For example, with regards to the question “Who is collecting your information? Where will the information end up?”, most of the participants from western countries and China both mentioned advertisers, software developers, social network platform such as Facebook and Instagram (mentioned by participants from western countries), or Weibo (mentioned by Chinese participants). None of the 43 Chinese participants mentioned the government, whereas 2 of the 17 participants from western countries proposed the possibility of government surveillance.

It is important to declare that the size of participants was relatively small and the comments made by participants were relatively subjective. However, to a certain extent, our finding suggests that the Chinese participants tend to rely on the government to protect their privacy and mainly care about invasions of privacy by big corporations. The participants from western countries, by contrast, were concerned about the disclosure of personal information to corporations, as well as to government.

## 5 Discussion

We have reported the results of a user study that investigates the trade-off between privacy and utility in mobile services. The research explored the human factors that influence the decision-making process pertaining to the trade-off and reported the major concerns of adopting privacy-preserving technologies. In addition, the research explored the cultural differences regarding the protection of privacy with participants from the UK and China as an example. Our findings enhanced the theoretical understanding of privacy concerns in this emerging area and provided practical suggestions for stakeholders involved in this context.

Our findings suggest that human factors such as users’ understanding of privacy risks, users’ trust of service providers, users’ desire for mobile services, and their belief

of cyber privacy are all important contributing items of the decision-making process. Meanwhile, users are also encouraged to share their information in particular situations.

Most participants expressed a strong desire for adopting privacy-preserving technologies in this context. While there is a potential to establish a win-win situation for users and mobile service providers, participants also showed their concerns about the potential trouble that might be caused by adopting such technologies, including learning cost, frequent reminders, and — a major concern — the need for a governing body to monitor the activities of technology providers. Most Chinese participants stated that government should play such a role; this was less popular with western participants.

This study confirms several findings from the existing research on privacy issues of mobile services. First, this research presented and investigated the human factors that influence the decision-making process pertaining to the trade-off between privacy and utility in mobile services. This advances our understanding of mobile users' behaviour and the potential causes of the privacy paradox. Future research can expand and weigh the factors to build related models. Second, our findings suggested that, although users are aware of their privacy leakage, an appropriate compensation mechanism could still encourage them to get involved in the privacy-trading process. To this end, if users are given corresponding rewards, as well as the ability to make independent choices with regards to releasing specific parts of their personal information, they are more likely to adopt the exchanging relationship with service providers. From this perspective, future research can explore potential strategies to provide mutual benefits for both sides of the trade. Third, this research enhanced the theoretical understanding of the differences of privacy concerns from cross-cultural dimensions. Future research can be conducted to further study the effects of culture on privacy concerns.

This study provides guidelines for mobile service providers who are interested in improving trust to help recruit more privacy-sensitive users. It also shows the direction that might be followed to foster adoption of privacy-preserving technologies to help mobile users in their attempts to balance privacy and utility. First, practical suggestions for mobile service providers or app developers can be provided by examining the factors discussed in this paper. For example, strategies such as providing a statement regarding how users' information is going to be used in apps, using data in only aggregate form, or providing valued-added service and coupons can effectively encourage users to release the information and apply the related mobile services. Second, the findings suggested that more attention should be paid to enhancing users' trust in privacy-preserving technologies. Although the benefits of applying such technologies are clear, users' distrust can negatively affect the adoption. Third, our findings suggested that, with regards to the role of supervising privacy-preserving technologies, none of the government departments, non-governmental organisations or large companies can in isolation obtain users' trust. It would appear that a mechanism that involves all of these stakeholders would be most palatable.

As with any empirical research, our study has limitations. First, the number of participants is relatively small and the participants themselves have a degree of imbalance: the total number of participants is 60, with 17 participants from western countries and 43 participants from China. (Although there are precedents: in a previous study, 22 people working in the IoT field were interviewed in Finland and in China (11 people

respectively) to investigate their different personal perspectives on individual privacy in the IoT [28].) Second, the main participants in our research are young adults — most of whom had received undergraduate or post-graduate education. A future study will give consideration to a broader range of users. Third, the factors and their importance provided by participants are relatively subjective. Again, a larger sample in future work will inevitably help to mitigate such subjectiveness.

## Acknowledgments

The authors thank the participants of the survey for their valuable comments. We are grateful to the reviewers for their constructive and helpful comments. We also wish to thank Norbert Nthala, Emma Osborn and Aaron Ceross for discussions that helped to improve this work. Yang Liu is supported by the National Key Research and Development Program (2017YFB0802204) and Basic Research Project of Shenzhen, China (JCYJ20180507183624136).

## References

1. AppBrain. Google Play Stats. <http://www.appbrain.com/stats>, 2017. [Last accessed December 2017].
2. G. Bal, K. Rannenberg, and J. Hong. Styx: Design and evaluation of a new privacy risk communication method for smartphones. In *Proceedings of the 29th IFIP International Information Security Conference (IFIP SEC 2014)*, pages 113–126. Springer, 2014.
3. S. B. Barnes. A privacy paradox: Social networking in the united states. *First Monday*, 11(9), 2006.
4. Z. Benenson, A. Girard, and I. Krontiris. User acceptance factors for anonymous credentials: An empirical investigation. In *Workshop on the economics of information security (WEIS2015)*, 2015.
5. A. R. Beresford, D. Kübler, and S. Preibusch. Unwillingness to pay for privacy: A field experiment. *Economics Letters*, 117(1):25–27, 2012.
6. J. L. Boyles, A. Smith, and M. Madden. Privacy and data management on mobile devices. *Pew Internet & American Life Project*, 4, 2012.
7. R. Cooper, H. Assal, and S. Chiasson. Cross-national privacy concerns on data collection by government agencies. In *Proceedings of the 15th International Conference on Privacy, Security and Trust (PST)*, pages 28–30, 2017.
8. J. B. Eap and D. Baumer. Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM*, 46(4):81–83, 2003.
9. R. L. Gorden. *Interviewing: Strategy, techniques, and tactics*. Dorsey press Homewood, IL, 1969.
10. S. Holavanalli, D. Manuel, V. Nanjundaswamy, B. Rosenberg, F. Shen, S. Y. Ko, and L. Ziarek. Flow permissions for Android. In *Proceedings of the 28th IEEE/ACM International Conference on Automated Software Engineering (ASE 2013)*, pages 652–657, Palo Alto, CA, USA, 2013. IEEE.
11. I. Kayes, N. Kourtellis, D. Quercia, A. Iamnitchi, and F. Bonchi. Cultures in community question answering. In *Proceedings of the 26th ACM Conference on Hypertext & Social Media (HT 2015)*, pages 175–184. ACM, 2015.

12. M. J. Keith, S. C. Thompson, J. Hale, P. B. Lowry, and C. Greer. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies*, 71(12):1163–1173, 2013.
13. M. Kern and J. Sametinger. Permission tracking in Android. In *Proceedings of the 6th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM 2012)*, pages 148–155, Barcelona, Spain, 2012.
14. J. Kitzinger. Qualitative research. introducing focus groups. *BMJ: British Medical Journal*, 311(7000):299, 1995.
15. F. Liu, X. Zhao, P. Y. Chau, and Q. Tang. Roles of perceived value and individual differences in the acceptance of mobile coupon applications. *Internet Research*, 25(3):471–495, 06 2015.
16. Y. Liu and A. C. Simpson. Privacy-preserving targeted mobile advertising: Formal models and analysis. In *International Workshop on Data Privacy Management (DPM 2016)*, pages 94–110. Springer, 2016.
17. Y. Liu and A. C. Simpson. Privacy-preserving targeted mobile advertising: Requirements, design and a prototype implementation. *Software: Practice and Experience*, 46(12):1657–1684, 2016.
18. X. Luo, H. Li, J. Zhang, and J. P. Shim. Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision support systems*, 49(2):222–234, 2010.
19. G. Marvin. Survey: 3 out of 4 consumers now notice retargeted ads. <http://marketingland.com/3-out-4-consumers-notice-retargeted-ads-67813>, 2016. [Last accessed July 2017].
20. S. Okazaki and F. Mendez. Exploring convenience in mobile commerce: Moderating effects of gender. *Computers in Human Behavior*, 29(3):1234–1242, 2013.
21. C. Phelan, C. Lampe, and P. Resnick. It’s creepy, but it doesn’t bother me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI ’16)*, pages 5240–5251. ACM, 2016.
22. S. Pötzsch. Privacy awareness: A means to solve the privacy paradox? In *IFIP Summer School on the Future of Identity in the Information Society*, pages 226–236. Springer, 2008.
23. S. Preibusch. Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 71(12):1133–1143, 2013.
24. A. Sabouri. On the user acceptance of privacy-preserving attribute-based credentials – a qualitative study. In *International Workshop on Data Privacy Management (DPM 2016)*, pages 130–145. Springer, 2016.
25. K. B. Sheehan. Toward a typology of internet users and online privacy concerns. *The Information Society*, 18(1):21–32, 2002.
26. V. F. Taylor and I. Martinovic. Securank: Starving permission-hungry apps using contextual permission analysis. In *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, SPSM ’16*, pages 43–52, New York, NY, USA, 2016. ACM.
27. V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas. Adnostic: Privacy preserving targeted advertising. In *Proceedings of the 17th Annual Network and Distributed System Security Symposium (NDSS 2010)*, San Diego, CA, USA, 2010.
28. J. Virkki and L. Chen. Personal perspectives: Individual privacy in the IoT. *Advances in Internet of Things*, 3(02):21, 2013.
29. R. Wash, E. Rader, and C. Fennell. Can people self-report security accurately?: Agreement between self-report and behavioral measures. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI ’17)*, pages 2228–2232. ACM, 2017.