Does the Presence of Privacy Relevant Information Affect App Market Choice?

Citation for published version:

Digital Object Identifier (DOI):
10.1145/3334480.3383078

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Does the Presence of Privacy Relevant Information Affect App Market Choice?

Abstract

While in most countries, Google Play and Apple App Store dominate, Chinese mobile phone users can choose among dozens of different app markets, which differ greatly in the information presented. This makes the Chinese mobile ecosystem a unique case study for investigating whether users actively choose app markets that conform to their preferences. We investigated this question in a survey of 200 Chinese users aged 18-49. Scenarios covered apps that require disclosure of different types of sensitive information (shopping, dating, health), with gaming as a baseline. Users preferred markets that were easy to use and had a wide choice of apps. Only nine users highlighted security as a feature. Despite this, they primarily used only one app market—the pre-installed one. App-market specific features were important for the game scenario, but less important for all others. We suggest that download decisions for most apps are made before users enter an app market, and discuss implications for presenting privacy and security information.

Author Keywords

app markets; privacy; security; understanding users.

CCS Concepts

•Human-centered computing → Empirical studies in ubiquitous and mobile computing; •Social and profes-
sional topics → Cultural characteristics; • Security and privacy → Usability in security and privacy;

Introduction
In many countries, there are only two dominant app markets: Google Play for Android phones, and Apple App Store for iPhones. China is different. Since Google Play is not routinely installed on Chinese Android phones, dozens of alternative app markets have emerged. The biggest markets are typically maintained by established Internet companies, such as Baidu or Tencent, or by mobile phone manufacturers, such as Huawei and Xiaomi [13, 12]. These app markets differ greatly in the information they present to users, the security and quality checks they conduct on the apps in their store, and the number of apps provided [12]. There is a wealth of work on dashboards and interfaces to support users in making app download decisions that take into account their privacy preferences [2, 3, 8, 11]. Relevant information includes whether an app has ads, what the app’s privacy policy is, or what access permissions it needs. While no Chinese app market explicitly implements these results, some app markets are better at providing relevant information than others. In this study, we examine to what extent users actively choose markets that have more security relevant information.

Method
App Markets Used in the Study
For the purpose of our study, we selected 15 representative app markets, including 2 official app markets (Apple App Store and Google Play), the top 3 app markets maintained by large Chinese Internet companies (Tencent, Baidu and 360), the top 5 app markets provided by smartphone vendors (OPPO, Xiaomi, Meizu, Huawei and Lenovo), and 5 specialized third-party app markets (25PP, Wandoujia, Hi-

Table 1: Participant Demographics. Participants were able to choose multiple occupations, and some listed two personal phones.
The scenarios were designed to vary by the need to disclose sensitive personal information (health, dating), and by the need to disclose payment information (online shopping, health). Gaming served as a baseline. The two health scenarios were presented in two different versions, non-stigmatising (generic cold symptom: very bad cough) and stigmatising (symptom occurring near the genital area: painful urination). For half of the participants, the doctor scenario was assigned to the stigmatising condition, and the medication scenario to the non-stigmatising condition; for the other half, this was reversed.

Participants then indicated how likely they were to download an app given seven different criteria, which were chosen to reflect key differences between Chinese app markets as identified in [12]. Three of the seven criteria reflect curation (passed manual inspection, high quality rating, app is up to date), two provide relevant user data from the app market (high number of downloads, high average user rating), and the final two are properties of the app (contains in-app purchases, contains ads). Participants answered on a four-point Likert scale, where 1 corresponds to very likely, 2 to somewhat likely, 3 to somewhat unlikely, and 4 to very unlikely to download app with the criterion).

From the security and privacy point of view, users should ideally avoid apps that contain ads, which is of concern in particular for health apps [9]. They should also ensure that they have the latest version, which is likely to contain patches for known security issues.

The survey was designed in English, implemented on Qualtrics, and translated into Chinese. Since Chinese survey websites that provide access to balanced samples require use of their own survey tools, which have fewer functions, we recruited participants through personal networks and posts on the platform WeChat. They were reimbursed with RMB30 through WeChat Pay. This sum was established as a fair incentive by consulting with people who had previously taken and distributed surveys in China. We sampled both Android and Apple iPhone users. The study was certified with the Ethics Panel of the School of Informatics, University of Edinburgh, reference number 2019/60328.

Analysis

Differences in demographics between groups were assessed using Fisher tests and Kruskal-Wallis tests. Differences in judgements across scenarios were assessed using the Friedman test. The Nemenyi method, which is conservative in its calculation of significance, was used for assessing pairwise differences. The threshold for statistical significance was set conservatively at 0.01. We used the implementation provided in the R Package PMCMR.

Free comments on markets (use, why, likes, dislikes) were analysed using content analysis. One of the authors extracted key issues and designed the initial code book. A second author then checked and revised the code book, and final annotations were completed based on the revised code book.

Results

Participants

We received 217 responses, of which 17 were excluded due to invalid responses on the personality and privacy scales. This leaves a total of 200 participants. Two thirds were female, most were aged below 30, and two thirds were employed. A third were students. Most of the employed participants had completed a university degree, which means that our participants were overall highly educated. While there were no gender differences by age, students were less likely to be female.
Table 2: Percentage of respondents who know, use, or frequently use an app store.

<table>
<thead>
<tr>
<th>Store</th>
<th>Known At All</th>
<th>Used Frequently</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple App Store</td>
<td>196</td>
<td>127</td>
</tr>
<tr>
<td>Google Play</td>
<td>170</td>
<td>58</td>
</tr>
<tr>
<td>Tencent</td>
<td>190</td>
<td>71</td>
</tr>
<tr>
<td>Baidu</td>
<td>190</td>
<td>69</td>
</tr>
<tr>
<td>360</td>
<td>190</td>
<td>71</td>
</tr>
<tr>
<td>Huawei</td>
<td>191</td>
<td>68</td>
</tr>
<tr>
<td>Xiaomi</td>
<td>189</td>
<td>52</td>
</tr>
<tr>
<td>Meizu</td>
<td>182</td>
<td>25</td>
</tr>
<tr>
<td>Lenovo</td>
<td>169</td>
<td>20</td>
</tr>
<tr>
<td>OPPO</td>
<td>183</td>
<td>36</td>
</tr>
<tr>
<td>X25PP</td>
<td>128</td>
<td>10</td>
</tr>
<tr>
<td>Wandoujia</td>
<td>176</td>
<td>42</td>
</tr>
<tr>
<td>HiApk</td>
<td>146</td>
<td>27</td>
</tr>
<tr>
<td>AnZhi</td>
<td>119</td>
<td>8</td>
</tr>
<tr>
<td>LiQU</td>
<td>117</td>
<td>7</td>
</tr>
<tr>
<td>Other</td>
<td>154</td>
<td>32</td>
</tr>
</tbody>
</table>

Four in five respondents check their mobile phone every hour (c.f. Table 1); there are no differences in age, gender, or occupation between those who do and those who do not. The average score on the privacy scale was 52 (SD: 8, range: 33–63). Participants felt quite strongly about their privacy, and most were fully aware of their personal data being tracked and collected.

All users had social and communication apps installed on their phone, and 92% reported using them frequently. Two thirds often use shopping apps, but only a quarter reports frequent mobile gaming. 68% do not have any health apps installed on their private phone, and if they do, they use them rarely.

<table>
<thead>
<tr>
<th>Brand</th>
<th>Users</th>
<th>Brand Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>97</td>
<td>87 (90%)</td>
</tr>
<tr>
<td>Huawei</td>
<td>58</td>
<td>41 (71%)</td>
</tr>
<tr>
<td>Redmi</td>
<td>20</td>
<td>11 (50%)</td>
</tr>
<tr>
<td>OPPO</td>
<td>9</td>
<td>3 (33%)</td>
</tr>
<tr>
<td>Smartisan</td>
<td>2</td>
<td>2 (100%)</td>
</tr>
<tr>
<td>Other</td>
<td>15</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>

Table 3: Percentage of respondents who often use the app store associated with the brand of their own phone.

Information Preferences
Users are very likely to download an app (median rating: 1) if it has high user ratings, somewhat likely (median: 2) if it is up to date, has passed manual inspection, is of high quality, or has a high number of downloads, and somewhat unlikely (median: 3) if it contains ads.

The app features that matter to users do not vary much across scenarios. The main difference is between gaming and dating: Users are more likely to value a larger number of downloads ($p < 0.005$), higher quality ratings ($p < 0.005$), higher user ratings ($p < 0.0005$), and being up to date ($p < 0.0005$) when choosing a new game. Users also tend to prefer apps that allow them to make in-app purchases when looking for medical advice ($p < 0.0005$) or purchasing medication ($p < 0.00001$) as opposed to gaming. We found no effect of potential stigma on users’ preferences for health apps. Ads always affect download decisions negatively, and human inspection always affects decisions positively.

Market Choice Inertia
Participants are aware of almost all markets mentioned in the questionnaire (median: 14, inter-quartile range: 10–15), but rely on a single app market for most downloads.
(median: 1, inter-quartile range 1–1), even though they have a median of two markets installed on their phone (inter-quartile range: 1–5). Those with a phone from Apple, Huawei, Redmi, and Smartisan tend to use the app market that is associated with their mobile phone; users of OPPO and other Android phones tend to use other app markets (c.f. Table 3). 32 participants mentioned other ways of obtaining apps, including the market associated with their own phone that was not mentioned in the survey (Smartisan), independent markets such as TapTap, downloading apps from the browser, and copying installation files (APKs) directly onto their phone. One user stated that there was no need for app markets, since all apps already came with their phone.

The Apple App Store and the Huawei App Store are the only stores with more than 20 frequent users in our sample. All other stores, including well-known third party stores such as TenCent, are used far less often (c.f. Table 2). Note users answered the question about app market use for all of their phones, which explains the higher numbers in Table 2 compared to Table 3.

193 participants gave reasons for their choice of main app market. Two of them reflected system constraints: the app market came with the phone operating system (n=136 mentions, 70%), and the phone could not be jailbroken (n=14, 4%) to allow for the installation of other app markets, which was primarily a concern for iPhone users. The next most important aspect was ease of use (n=60, 31%), followed by privacy related reasons, including the absence of ads (n=27, 14%), and the number of apps available (n=20, 10%). The final set of reasons (no other markets known, popularity, less download traffic) were only mentioned rarely.

190 participants told us what they liked or disliked about app markets. Problematic issues included unavailability of apps (n=41, 22%), ads (n=27, 14%), bad user experiences (n=21, 11%), slow speed (n=14, 7%), cost (n=11, 6%), and app recommendations (n=11, 6%). Nine users (5%) complained about security issues. A third of the respondents (n=57, 30%) were neutral about app markets; they used them because they had been provided with the phone. Positive aspects included ease of use (n=29, 15%) and range of apps available (n=23, 12%).

**Discussion and Conclusion**

We found strong user preferences for the app market installed on their phone, even though the most common Android App market, Huawei’s, does not provide information about privacy policies, quality ratings, and in-app purchases, which are provided by vendor-independent alternatives. This accurately reflects the main reason users gave for choosing their main app market, and might be another instance of the well-known gap between users’ privacy preferences and their privacy behaviour (see e.g. [10] for the disclosure of sensitive information). We obtained these results even though participants had been primed to think about privacy by administering the privacy questionnaire before the scenarios, and even though participants were well educated, of relatively high socioeconomic status, and valued online privacy. If there is one group of users that we would expect to actively choose app markets, it is this one.

The pattern of responses we have seen, which is backed up by our qualitative findings, suggests that the main app selection decisions are made outside of the app markets. This is in line with the findings of Kelley et al. [8] that the information in their privacy dashboard had a significant, but small effect on app choice. We suspect that participants are unlikely to switch to an app market with strong app security checks and transparent privacy dash boards, unless those features are easy to use, and there is a broad range
of apps available. Indeed, HiAPK is the only market represented that does not check copyright, check apps, or perform security checks [12]. Yet, it is the second most used among the five specialised app markets (c.f. Table 2).

There are two important confounding factors that we did not assess in this questionnaire: the role of privacy and mobile computing self-efficacy (e.g. [7, 1]), and the role of pre-app market research in app selection. The effect of additional information in the app market might be the strongest for games, because there are so many games in the market, such that users face a real choice, while the choice of apps for shopping, dating, ordering medication and consulting with doctors is a lot more narrow, and users might prioritise the ability to download their app of choice over other attributes.

In future work, we aim to conduct user interviews in order to better understand the dynamics of app and app market selection, and the stage of app selection at which privacy and security are considered. We also intend to contextualise our findings with a narrative review of what is known about Chinese users’ privacy preferences, privacy strategies, and privacy self-efficacy. Last, but not least, this pilot survey only covered 200 relatively well-educated participants. We plan to test the working hypotheses discussed above in a larger study with a more socio-demographically balanced sample.

Acknowledgements
We thank our participants for their time, and the reviewers of the previous version of this paper for their valuable in-depth feedback. MW’s contribution was supported by the Alan Turing Institute (EPSRC, EP/N510129/1). HW and YG were supported by the National Natural Science Foundation of China (No.61702045 and No.61772042).

REFERENCES


