Mobile privacy: users’ expectations about the behavior of mobile apps

Full Papers

Jose Santiago Moreira de Mello  
Computer Science Department  
Federal University of São Carlos  
jose.mello@dc.ufscar.br

Sergio Donizetti Zorzo  
Computer Science Department  
Federal University of São Carlos  
zorzo@dc.ufscar.br

Diego Roberto Gonçalves de Pontes  
Computer Science Department  
Federal University of São Carlos  
diegorobertogp@hotmail.com

Abstract

Many tools have been proposed in the literature to analyze the behavior of mobile applications regarding user data collection. However, these tools do not take into consideration the users’ perception of what they think is collected and the purpose of such collection. In this sense, this paper proposes a privacy approach applied to the mobile context that considers the users’ expectations about their data collection and usage on smartphones. This work presents results of an experiment conducted with 163 Android users which goal was to understand the users’ expectations regarding the behavior of mobile apps and how that impacts their subjective feelings. Our results suggest that most users did not know which of their private data were collected by mobile applications and tended to be more comfortable when they were informed beforehand which data a mobile app would need access to and why.

Keywords

Mobile privacy, Expectation, Android permission, Data privacy, Mobile application.

Introduction

In the last few years, smartphones have become a part of peoples’ daily routines and sparked the number of apps in this platform. The usage of these apps brings a large deal of advantages for users’ daily activities such as online banking, instant communication, socialization and leisure. One standard to measure the growth of this segment is the annual Internet Trends report, by Kleiner Perkins Caufield Byers (KPCB), and it indicates a 58% increase in the number of apps for mobiles in 2015. Google Play Store, the official app store for Android, surpassed the mark of 700,000 apps, free and paid, available to download in 2012 (Carbunar and Potharaju 2015).

Given this scenario, users’ private data is a concern because many of these apps handle (sometimes without the user’s knowledge) sensitive information such as approximate location, contact numbers and call logs. The users’ control over access to this information is rather limited or nonexistent, since it is not possible to negotiate the terms of data usage and handling in apps and many of them simply do not work without accessing the user’s data. In other words, in order to take advantage of the benefits of mobile apps, the user must agree to let them access his/her data.

Indiscriminate access to user data opens up breaches regarding security and privacy such as malicious code (malware) that takes advantage of vulnerabilities to collect user data (Felt et al. 2011). Another relevant problem is legitimate apps that gather user data without the user’s knowledge. As reported by the

Mobile privacy

New York Times\(^2\), the Facebook app used to copy users’ contact lists to their servers, which raised many questions about the real reason of this procedure.

Many works in the literature have proposed ways to protect the privacy of mobile users by using application analysis mechanisms such as those presented by (Chin et al. 2011; Enck 2011). Other works, like Beresford et al. (2011) and Hornyack et al. (2011), propose security extensions that help users know which of their data are collected and why. These mechanisms are useful to analyze the behavior of a mobile app. However, none of them assesses the users’ expectations about data collection and usage or how comfortable they feel about knowing details of which of their data are collected and the purpose of such collection.

In this paper, we approached privacy through the perspective people have regarding data collection and usage in mobile apps. To do so, we performed an experiment with users in order to assess their expectations and comfort levels about the behavior of mobile applications.

There are many discussions about the importance of expectations in a privacy context, as proposed by (Solove 2006). We believe that the idea of analyzing privacy based on users’ perception of apps behaviors can be achieved in two steps. The first one is related to performing an experiment to understand the users’ perception of the behavior of a mobile app. The second step is to analyze the real behavior of such apps and compare them to the expectations from the first step.

We believe that the access to certain data of a mobile device may imply access to users’ confidential and sensitive information. For example, an app that has access to GPS coordinates knows the user’s approximate location. Similarly, an app that has access to the user’s contacts (WhatsApp, for instance) knows what people are related to that particular user. So, when we assess the access to data on mobile devices we are also assessing the possibility of accessing confidential data that is handled by these apps.

Given this context, this paper presents the results of a research conducted with Android users that aimed to analyze the expectation users have under specific conditions regarding the behavior of mobile applications.

We highlight the following contributions of this research:

- We present a way to capture users’ expectations using an electronic survey. More specifically, we conducted a study with a group of 163 Android users and examined their expectations and subjective feelings about the behavior of different mobile applications that have access to data like their contact list and device ID.

- We point out two factors that affect the way people think about privacy in mobile apps: the expectation of what is being collected and to what end. We then show how these factors impact the users’ subjective feelings.

- We present an analysis that indicates that letting the user know why a given information is being used may relieve his/her concern about privacy, since most users have trouble finding out which of their data is being used and to what end.

**Related Works**

For the sake of a better understanding, the works related to this paper were divided into two sections: one is about Android’s access request mechanism and the other one is about mobile applications analysis techniques.

**Android’s access request mechanism**

The Android access request mechanism was developed based on two premises: (1) to limit mobile applications’ access to confidential information (e.g., contacts and location) and (2) to help users make trustful decisions before installing a given app. Android apps may only access data the user agrees to during the install process. In this process, a list of requested permissions required for the app to work is

shown to the user. Then the user must choose between installing the app with all its requests or not installing it, since the list of requests is non-negotiable.

There are many studies that assess the usability of this mechanism. A study conducted by (Kelley et al. 2012) used semi-structured interviews with Android users and noted that people have a limited attention span regarding request screens since they do not understand the real impact such permissions have on their privacy.

This lack of understanding makes it difficult for people without technical knowledge to have an opinion about the risk any given app may present to their privacy. In Kelley et al. (2012), the authors point out that most users make their decisions on trusting or not an app by analyzing how other users rated the app.

Similarly, Felt et al. (2012) assessed the usability of the Android access request mechanism focusing on the level of attention users have on warnings from this mechanism. The authors conducted a study with two groups of participants, one via internet and the other on-site, and concluded that, for both groups, the warnings of the Android access request mechanism were not effective on informing the privacy risk of installing a given app. One of the problems pointed out by the authors was the excessive amount of warnings, which made the users fatigued as well as made them give up on reading app policies and skipped to accepting the terms and installing the app.

Our work extends the ideas presented by Felt et al. (2012) and Kelley et al. (2012) by presenting a way to measure the users’ expectations about the behavior of mobile applications. This allows us to capture a new privacy aspect (data collection expectation and data collection purpose) that was not present in previous works.

Mobile applications analysis

Many researchers present useful techniques and tools to detect and notify mobile application data collection. The work of Poeplau et al. (2014) proposed a statistical analysis tool for mobile applications aimed at detecting calls of external codes that might be used to run malware on the user’s device and jeopardize his/her confidential data.

The statistical analysis assesses the application when it is not running. By doing so, the method tries to check for the need of using certain Application Programming Interfaces (APIs), which are known for collecting user data (for example, authentication APIs integrated with social networks). The statistical analysis also tries to assess if the application runs external codes such as a call to a webservice.

Another approach to analyze the behavior of applications is dynamic analysis. In this approach, the application is analyzed during its execution and data accessed by it are constantly monitored.

In this context, Enck et al. (2014) conducted a study in which they presented a tool called TaintDroid, a dynamic analysis system that is able to detect when a given application accesses data on the mobile device. The results presented by Enck et al. (2014) and Poeplau et al. (2014) showed excessive access to users’ confidential data, jeopardizing their privacy.

In our research, we used the TaintDroid tool to investigate the data access behavior of some applications and the purpose of this access. To do so, we selected a set of mobile applications and assessed them.

Our work follows the same premise in Enck et al. (2014) and Poeplau et al. (2014), which is to inform users about topics that concern their privacy. Our approach also includes the users’ expectations in this process.

Many other solutions to protect privacy of mobile users can be found in the literature. For example, MockDroid, proposed by Beresford et al. (2011) and Taming information-stealing smartphone applications (TISSA), presented by Zhou et al. (2011) are tools that replace calls made by APIs with false information. Even though many efforts were made to not affect the app’s execution with these replacements, there are reports that some applications are sensible to this procedure and do not perform well under this condition.

In this context, Melo and Zorzo (2012) proposed the Personalized User Privacy Mechanism for Android (PupDroid) that implements a mechanism that allows mobile device users to control data access of apps. This tool basically works by adding rules defined by the user about which applications can access which data on their mobile devices.
Study Design

The conduction of the experiment in order to obtain the users’ expectation was performed in a Higher Education Institute (Instituição de Ensino Superior – IES) in Ourinhos, southwest of São Paulo state. The participants of this research were selected from an invitation sent out to the IES’s mailing list.

We used an online system especially developed to conduct this experiment. After agreeing to a consent term, the participants were directed to a demographic survey screen in which they were asked to enter information such as age, gender and level of education. After that, a screen with a list of the top 10 most downloaded apps in Brazil in 2015 was shown (Annie 2015). Then the participants were asked to select which of those apps they use or have used, and given their selection a few questions were asked.

After selecting the apps, the participants were asked to check the app screenshots and description as presented in the Google Play Store. Then they were conducted to one of the two sets of questions shown in Figure 1. The first set (expectation group) was projected to capture the users’ perceptions and assess if they expected that a given mobile app would access a certain kind of data (for instance, the contact list). The participants who answered questions of this group also answered questions on why they thought the app would need access to that given data.

![Figure 1. Examples of questions for the purpose and expectation groups, respectively.](image-url)
The other set of questions, hereby referenced as the purpose group, was projected to assess how people felt when we provided more specific information about the app. In this step, participants were informed that a given data would be accessed by the application for specific reasons; for instance, access to the contact list is necessary to provide the main functionality of WhatsApp. We identified which data the app accessed by examining TaintDroid logs and analyzed the app’s privacy policy to understand why they needed access to those particular data.

For both sets of questions, we used a Likert scale of 4 points that varied from highly comfortable (+2) to highly uncomfortable (-2) to measure how comfortable users felt regarding the scenario presented by the questions.

The online survey system randomly divided the participants into two groups. The expectation group was comprised of 82 people and the purposed group was comprised of 81 people.

The separation into two groups was made in order to compare the perceptions and subjective feelings participants had when provided with relevant information about the apps’ behaviors.

To make our experiment viable, we opted to focus our analysis in 4 types of data accessed by the mobile applications, as suggested by Hornyack et al. (2011): contact list, IP address, approximate location (GPS) and mobile device ID. According to a study conducted by Hornyack et al. (2011), these data are the most used by apps.

The device ID represents access to any of the 4 elements used to uniquely identify a mobile device: International Mobile Equipment Identity (IMEI), Integrated Circuit Card Identifier (ICCID), International Mobile Subscriber Identity (IMSI) and the telephone number associated with the device’s SIM card.

We also restricted the set of apps analyzed to the top 10 most downloaded apps in the Google Play Store in Brazil in 2015 according to a report by (Annie 2015).

The experiment was conducted between November 21\textsuperscript{st} and November 25\textsuperscript{th}, 2016. We collected 554 answers; however, 38 were discarded because the participants closed the electronic questionnaire before finishing it. On average, each participant took approximately 82 seconds (Avg = 81.5 seconds and Std dev = 19.21 seconds) to answer the questions about each selected mobile application. The standard deviation was approximately 19 seconds. Considering only the valid answers, the distribution of gender and age of the participants are shown in Table 1.

<table>
<thead>
<tr>
<th>Gender</th>
<th>Participants</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>105</td>
<td>64.42</td>
</tr>
<tr>
<td>Female</td>
<td>58</td>
<td>35.58</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Age</th>
<th>Participants</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 to 20 years old</td>
<td>43</td>
<td>26.38</td>
</tr>
<tr>
<td>21 to 25 years old</td>
<td>53</td>
<td>32.52</td>
</tr>
<tr>
<td>26 to 30 years old</td>
<td>40</td>
<td>24.54</td>
</tr>
<tr>
<td>over 30</td>
<td>27</td>
<td>16.56</td>
</tr>
</tbody>
</table>

Table 1. Distribution of participants.
Results and Analysis

In our first analysis, we tried to identify which pairs <app, collected data> had the lowest data collection expectation by the participants. For each pair we gathered information from the questionnaires and calculated the percentage of participants who presented expectations aligned with the results from TaintDroid and the app’s privacy policy.

We also calculated the self-assessment average (comfort level) from participants’ answers. We used a range from +2 to -2, where +2 indicates “highly comfortable” and -2, “highly uncomfortable”.

An overview of the pairs <app, collected data> is shown in Table 2. At least 20% of the participants correctly assessed that a given app would need access to certain information. For example, only 15% of the participants correctly anticipated that YouTube requires access to users’ contact list. In general, these participants felt uncomfortable about this data collection. The average comfort level was -1.32.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Applications</th>
<th>Expected (%)</th>
<th>AVG Comfort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact list</td>
<td>YouTube</td>
<td>15%</td>
<td>-1.32</td>
</tr>
<tr>
<td></td>
<td>Clean Master</td>
<td>15%</td>
<td>-1.18</td>
</tr>
<tr>
<td>GPS location</td>
<td>Instagram</td>
<td>10%</td>
<td>-1.10</td>
</tr>
<tr>
<td></td>
<td>Snapchat</td>
<td>5%</td>
<td>-0.95</td>
</tr>
<tr>
<td></td>
<td>Skype</td>
<td>13%</td>
<td>-1.35</td>
</tr>
<tr>
<td></td>
<td>YouTube</td>
<td>7%</td>
<td>-1.12</td>
</tr>
<tr>
<td>Network address</td>
<td>Snapchat</td>
<td>15%</td>
<td>-1.19</td>
</tr>
<tr>
<td></td>
<td>Clean Master</td>
<td>15%</td>
<td>-1.30</td>
</tr>
<tr>
<td>Device ID</td>
<td>360 Mobile Security</td>
<td>9%</td>
<td>-1.09</td>
</tr>
<tr>
<td></td>
<td>UC Browser</td>
<td>5%</td>
<td>-0.90</td>
</tr>
<tr>
<td></td>
<td>Facebook</td>
<td>20%</td>
<td>-1.45</td>
</tr>
</tbody>
</table>

Table 2. Applications and resources with lower access expectations.

Similarly, only 10% of the participants correctly anticipated that Instagram requires access to the device’s GPS location and 20% correctly anticipated that Facebook requires access to the device’s ID.

In general, participants who were surprised about a particular data collection from an app rarely knew to what end that data would be used for.

It is important to note that this analysis covers the expectation group, whose participants were not informed neither about which data the apps accessed nor why. Under these conditions, we observed a strong negative correlation (r = -0.92) between the expectation percentage and the comfort average, both shown in Table 2.

In other words, the users’ perception about an app, the data it collects and their comfort levels are inversely related; so the higher the expectation users had about an app collecting their data, the lower was their comfort.

The correlation coefficient used in this study was calculated using Person’s r correlation, given by

\[
 r = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^{n} (y_i - \bar{y})^2}},
\]
where \( n \) is the number of elements in the analyzed set, \( x \) represents the percentage variable and \( y \) is a variable related to the average comfort metric.

**Users’ difficulties to identify purpose**

The analysis of the expectation group participants’ answers showed that, in general, these users have difficulties in identifying the reason why an app accesses some of their data.

We compared their answers with the results from TaintDroid regarding the apps’ actual behavior; we also analyzed the apps’ privacy policies. Then we manually categorized each \(<\text{app, collected data}>\) pair into four categories: (1) providing the main functionality, (2) profile usage analysis (traceability), (3) advertisements and (4) sharing with third-parties. Many of the data we analyzed fell under more than one category. For example, WhatsApp uses the user’s contact list to provide the main functionality, to analyze the user profile usage as well as to share it with third-parties.

We compared the answers of the expectation group participants with our analysis and the results are shown in Table 3. In most cases, the participants were not able to correctly point out the reason why an app needed access to some of their data.

Another important observation is that when user data was used to provide the app’s main functionality, participants scored higher. However, their grades never surpassed 65%.

We also observed that the device ID was the kind of data that had the most assertive answers when compared to others. When data was used to more than one purpose, the participants’ correct anticipation of it tended to be much lower.

A comparison between participants’ expectation versus the apps’ real behavior is shown in Table 3.

<table>
<thead>
<tr>
<th>Data</th>
<th>Purpose</th>
<th>Num. of apps</th>
<th>% Correct answers</th>
<th>% Do not know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact list</td>
<td>[1]</td>
<td>7</td>
<td>65%</td>
<td>9%</td>
</tr>
<tr>
<td></td>
<td>[3]</td>
<td>6</td>
<td>45%</td>
<td>38%</td>
</tr>
<tr>
<td></td>
<td>[2] + [4]</td>
<td>5</td>
<td>19%</td>
<td>28%</td>
</tr>
<tr>
<td>Approximate location (GPS)</td>
<td>[3]</td>
<td>7</td>
<td>44%</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>[1] + [2]</td>
<td>3</td>
<td>23%</td>
<td>32%</td>
</tr>
<tr>
<td></td>
<td>[4]</td>
<td>8</td>
<td>27%</td>
<td>19%</td>
</tr>
<tr>
<td>Network address</td>
<td>[1] + [3]</td>
<td>6</td>
<td>16%</td>
<td>22%</td>
</tr>
<tr>
<td></td>
<td>[2]</td>
<td>3</td>
<td>13%</td>
<td>37%</td>
</tr>
<tr>
<td></td>
<td>[4]</td>
<td>8</td>
<td>38%</td>
<td>46%</td>
</tr>
<tr>
<td>Device ID</td>
<td>[3]</td>
<td>6</td>
<td>41%</td>
<td>26%</td>
</tr>
<tr>
<td></td>
<td>[4]</td>
<td>7</td>
<td>22%</td>
<td>33%</td>
</tr>
<tr>
<td></td>
<td>[1]</td>
<td>10</td>
<td>62%</td>
<td>11%</td>
</tr>
<tr>
<td></td>
<td>[2]</td>
<td>9</td>
<td>20%</td>
<td>27%</td>
</tr>
</tbody>
</table>

Table 3. Comparison between expectation and actual behavior of apps.

The first column shows the type of data that was accessed and the second column shows the results from TaintDroid along with privacy policy analysis.

To make it easier to visualize the type of data that was being accessed, we created indications to represent the purpose why a particular datum was used. These indications are [1] providing the main functionality, [2] profile usage analysis, [3] advertisements and [4] sharing with third-parties.
The third column shows the number of apps that fell under that category. For example, in the first row of Network address, 6 apps accessed the contact list to provide their main functionality (1) and to advertise (3).

The fourth column shows the percentage of participants that correctly identified the purpose behind a particular datum access. And finally, the fifth column shows the percentage of participants that said they did not know why that particular datum needed to be accessed.

**Clarifying purpose may mitigate users’ concerns**

Due to the lack of clarity as to why their mobile device data is used for, users often have to deal with significant levels of uncertainty in the decision making process of installing and using a mobile app.

In our study, we wanted to observe if offering detailed and specific information about the reason why a particular app needs access to users’ data would have any influence on their feelings towards their privacy. To do so, we compared the average levels of comfort of both groups (purpose and expectation) for each <app, collected data> pair.

We observed that all 4 types of data we studied (contact list, approximate location (GPS), network location and device ID) had significant variations on the participants’ level of comfort. In general, they felt more comfortable when they were informed why an app needed access to some of their data.

This analysis is shown in Table 4. The most significant difference between the comfort levels is on the contact list. For all types of data, the average comfort levels of participants in the purpose group were higher than those in the expectation group.

<table>
<thead>
<tr>
<th>Data</th>
<th>Avg. comfort Expectation group</th>
<th>Std Dev Expectation group</th>
<th>Avg. comfort Purpose group</th>
<th>Std Dev Purpose group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact list</td>
<td>-0.88</td>
<td>1.19</td>
<td>-0.22</td>
<td>1.51</td>
</tr>
<tr>
<td>Network location</td>
<td>-0.63</td>
<td>1.43</td>
<td>-0.08</td>
<td>1.46</td>
</tr>
<tr>
<td>Approximate location (GPS)</td>
<td>-0.37</td>
<td>1.66</td>
<td>-0.15</td>
<td>1.45</td>
</tr>
<tr>
<td>Device ID</td>
<td>-0.46</td>
<td>1.63</td>
<td>-0.11</td>
<td>1.50</td>
</tr>
</tbody>
</table>

**Table 4. Comparison between levels of comfort.**

These results suggest that informing users about the reason an app needs access to their data not only helps them better understand how the app works and make better decisions, but it also mitigates their concerns that arise from not knowing what happens to their data.

The differences between the average comfort for both groups were significant for all types of data. Again, the comfort classification varied from -2 (highly uncomfortable) to +2 (highly comfortable).

**Discussion**

An important observation in this work is related to the subjective feelings participants had during the experiment. In general, they felt more comfortable when they knew the reason why a certain app needed access to their data.

There were some cases where apps accessed data that was not necessarily related to their main functionality. For example, Facebook access the users’ network address (IP) and shares it with third-parties. This fact conflicted with the expectation some participants had regarding apps like this, since most of them did not expect this particular data would be collected. Those who already expected this thought it would either be for advertisement or user profile analysis purposes. Due to this, they had a
much lower comfort level when compared to participants who were informed beforehand the reason why their data would be collected.

We also observed that there were cases where participants correctly expected the apps would access their contact list in order to provide their main functionalities (for example, the 360 Mobile Security app). However, their comfort levels were lower when compared with participants who were not informed beforehand the apps would collect data from their contact list. This result suggests that when dealing with uncertainties, users tend to be more concerned about something that may affect their privacy.

Currently, the Android permission screen that is shown when we want to install a mobile app does not have any specifications about why the app needs access to that data. This is a condition similar to the expectation group in this study. As mentioned before, informing the users why the app needs access to that data can help them make better decisions and, to some extent, even improve their comfort level about the app. A possible approach that users can make use of today is to use feedback from other users to verify how comfortable they were by installing a particular app.

**Concerns about advertisements**

We observed that apps that collect user data for advertisement purposes are a major concern among users. Given all 4 types of data we assessed in this study, advertisement was the type users felt more uncomfortable with.

We understand that many companies depend on publicity to monetize their applications. However, in order to improve user experience, they could consider informing them how and why their data is collected. This may help users get a better grasp of what the app is doing without compromising the quality of the advertisement service. Other approaches involve using tools to mask users’ real data by using substitutions, hash or cryptography, similar to what MockDroid and TISSA do. These techniques may help keep user data private, but may also cause some apps to malfunction.

**Conclusion**

Many works in the literature present significant contributions to the privacy and security fields, especially those aimed at providing automatic analysis tools to help users control their privacy. Nonetheless, none of these tools provide a mechanism that is able to distinguish if a particular data collection is necessary or how the uncertainty of not knowing the reason their data is being collected impacts users.

This paper presented an approach to explore privacy in mobile applications taking into consideration the users’ expectations. In our context, we explored the subjective feelings each user had about the expectation of apps accessing their data.

Our results suggest that both expectation of data usage and purpose of data usage have a great impact on users’ feelings and may affect their decision-making process. Another important observation is that when users are correctly informed about the access to a certain type of data and its reason, it can, to some extent, mitigate their concerns about their privacy.

The future goals of the research evolve the construction of an automatized system which brings up to the interested users the experiment participants’ main divergences related to the expectations and the app real behavior.

This device allows to amplify the results of this essay to different contexts, as evaluating different participants’ profiles and other types of mobile apps, since it also permits the interested users to contribute by answering electronically a questionnaire which is similar to the one presented previously, allowing replies to other non-evaluated apps on the original experiment.

We believe such mechanism is able to help users make confident decisions on the use (or not) of mobile apps which manipulates their information. This work can be considered the first step, presenting a way to acquire from the users their perceptions about which resource of the mobile apps are accessed and why the apps would need that access to the resource.
The control variable used on this research have been defined statically, according to what is suggested on literature (e.g., Hornyack et al. 2011), future researches will focus on using dynamic control variables which would permit the evaluation of the users’ perception on other contexts views besides mobile apps.

REFERENCES


