"It's Shocking!": Analysing the Impact and Reactions to the A3: Android Apps Behaviour Analyser

Majid Hatamian, Agnieszka Kitkowska, Jana Korunovska, Sabrina Kirrane

"It's shocking!": Analysing the Impact and Reactions to the A3: Android Apps Behaviour Analyser

Majid Hatamian[1⋆], Agnieszka Kitkowska[2], Jana Korunovska[3], and Sabrina Kirrane[3]

[1] Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, Frankfurt am Main, Germany,
majid.hatamian.h@ieee.org,
[2] Karlstad University, Karlstad, Sweden,
agnieszka.kitkowska@kau.se,
[3] Vienna University of Business and Economics, Vienna, Austria,
{sabrina.kirrane, jana.korunovska}@wu.ac.at

Abstract The lack of privacy awareness in smartphone ecosystems prevents users from being able to compare apps in terms of privacy and from making informed privacy decisions. In this paper we analysed smartphone users' privacy perceptions and concerns based on a novel privacy enhancing tool called *Android Apps Behaviour Analyser (A3)*. The *A3* tool enables user to behaviourally analyse the privacy aspects of their installed apps and notifies about potential privacy invasive activities. To examine the capabilities of *A3* we designed a user study. We captured and contrasted privacy concern and perception of 52 participants, before and after using our tool. The results showed that *A3* enables users to easily detect their smartphone app's privacy violation activities. Further, we found that there is a significant difference between users' privacy concern and expectation before and after using *A3* and the majority of them were surprised to learn how often their installed apps access personal resources. Overall, we observed that the *A3* tool was capable to influence the participants' attitude towards protecting their privacy.

Keywords: smartphone ecosystems; android; privacy; permission; privacy concern; privacy behaviour

1 Introduction

In the last decade, the privacy of data users/owners has become a growing concern due to the massive increase in personal information utilised in smartphone apps [1], social networks [2], outsourced search applications [3, 4], etc.

⋆ The authors would like to thank: A. K. Lieberknecht, C. Stern, H. Chen and Y. Obreshkov that partially contributed in the data collection task. This research work has received funding from the H2020 Marie Skłodowska-Curie EU project "Privacy&Us" under the grant agreement No 675730.

Smartphone apps are designed with consideration for the demands and constraints of the smartphones and to take advantage of any specialised capabilities that they have. The smartphone apps market is rapidly growing. In 2017, the total number of iOS and Android apps available on their marketplace were 2.2 and 3.5 millions, respectively [5]. Furthermore, the number of mobile app downloads has grown to 197 billion worldwide in 2017, which is almost 50 billion more than 2016 [6]. Such enormous number of apps available and the high number of downloads resulted in increased dependency on apps. In 2017, eMarketer released a study showing the average amount of time people spent using apps is two hours, 25 minutes per day [7]. The Techcrunch's report showed that on average, smartphone owners used nine apps per day and 30 apps per month. Accordingly, it was argued that smartphone users rely heavily on apps [8]. For instance, Marketing Land [9] reported that the smartphone users spent 86% of their internet usage time using apps. As a result, the landscape of smartphone use today is very much app-focused. All of these factors make smartphones an attractive target for privacy invasion.

Each app can request a certain number of permissions which allows it to gain access to the device resources such as contacts, location, storage, camera, etc. In older Android versions (prior to version 6.0), users had to grant permissions requested by each app at the install time and they were not able to restrict those permissions later. However, with the release of Android 6.0, the users were given control, and they are able to restrict the requested permissions even at runtime. Although this feature enables users to better preserve their privacy, prior studies have shown that few users are aware of it, hence permissions are often ignored even though they might appear irrelevant to the real functionality of the app [10]. This is due to the fact that many users do not understand the technical and sometimes ambiguous definitions of permissions [11]. Additionally, most of them value the use of the apps more than their personal information, despite the fact that the apps collect large amounts of personal information, for various purposes ranging from functionality to empower their ads mechanisms [12, 13].

The invasive nature of smartphone apps, harvesting personal data has been demonstrated in many studies. The Wall Street Journal reported a study in which 101 popular smartphone apps were examined for personal information gathering activities. Their results showed that more than half of the apps exhibited at least one risky behaviour, such as location tracking, transmission of a smartphone's unique device ID number, or the gathering of other personal information [14]. A report by Appthority showed that 95% of the top 200 free apps and 80% of the top paid apps for Apple and Android phones did the same [15]. Chia et al. [16] studied risk signaling concerning the privacy intrusiveness of Android apps in two repositories. Their results showed that the number of dangerous permissions an app requested was positively correlated with its popularity. Therefore, the fact that an app is popular does not imply that it respects users' privacy.

This paper presents the results of interviews and surveys of 52 participants who used our privacy enhancing tool called *Android Apps Behaviour Analyser*

(A3) that is solely designed and implemented for Android devices. In this study, we examine, compare and contrast smartphone users' concern and expectation, by leveraging a user study as a reference point for understanding smartphone-specific concerns and perceptions. This study is aimed to (1) propose a privacy enhancing tool for smartphone users to support them for informed privacy decision-making, (2) test our hypothesis that smartphone users are willing to take action and change their privacy attitude once they realise how their personal resources are treated by their installed apps, and (3) provide data over the understanding of users' privacy concern and expectation in using smartphone apps.

The rest of the paper is organised as follows: Section 2 reviews the existing works in the literature related to the privacy concern and expectation analysis of smartphone users. Section 3 describes the main concepts associated to the *Android Apps Behaviour Analyser (A3)* as a novel privacy enhancing tool for Android users. Section 4 presents the research steps and design decisions taken in the implemented user study to analyse the impact of *A3* on the users' privacy concern and expectation and the obtained results are then presented in Section 5. Finally, we conclude the paper and point the future directions of research in Section 6

2 Related Work

Kelley et al. [17] tried to identify possible causes and incentives for users to willingly share their location with advertisers. The results showed that users were highly concerned about their personal data. Almost 80% (19 out of 24) of the people questioned expressed the highest level of concern towards an unsolicited transfer of personal data gathered about them by a company on a corporate level (e.g. to other companies, institutions, governments, etc.). The authors concluded that the users are least concerned when they share information about being at certain pre-selected locations. The study suggested that this could be attributed, in part to the fact, that users may like being informed regarding certain promotion activities or other similar events related to the places specified (e.g. coupons for favourite restaurants). Differently, Erika et al. [18] studied overall privacy and security expectations of the users in choosing apps. They first surveyed 60 smartphone users to measure their willingness to perform certain tasks using their smartphones to test the hypothesis that people currently avoid using their phones due to privacy and security concerns. Second, they investigated why and how the users trust a certain app. The results showed that users are more concerned and conservative about privacy on their smartphones than their laptops. The authors also identified the threats which scare smartphone users of using smartphones (e.g. malicious apps, data loss, etc.). Based on these results, they suggested some recommendations to ameliorate privacy and security confidence of users to increase trust in choosing apps. A different user-centric study was published by Felt et al. [19]. They presented a risk ranking of sensitive smartphone resources by user concerns. A successive open-end enquiry among

a group of 42 participants gathered personal descriptions and ratings of a subset of evaluated risks which disclosed that the lowest-ranked risks are seen as disturbances, the highest-ranked risks however represent serious issues. They found that warnings in Android and iOS do not satisfy users' concerns. They concluded that future permission systems should consider user concerns when deciding which permissions are protected with warnings.

Lin et al. [10] investigated privacy expectations of smartphone users. The main goal of the authors was to figure out when an app violates users' expectations. Having considering this and by arguing that if a user's mental model aligns with what the app actually does, the authors claimed there would be fewer privacy issues since the user is adequately informed of the actual app's behaviour. This brought them to the point of allowing users to see the most common misexpectations about an app by revising users' mental model. For this reason, they suggested the use of both crowdsourcing users' mental models and profiling mobile apps using log analysis tools. Amini et al. [20] employed crowdsourcing as part of a procedure to analyse mobile apps privacy expectation. Participants were asked to rate their expectation and comfort feeling according to the access of sensitive information related to the identified tasks. Thus, by considering the context of apps as well as privacy invasive behaviour, an assessment of the desirability of this information leakage can be depicted. Continuing this work, Amini et al. [21] envision the tool *AppScanner*, consisting of different sub-modules, to be able to evaluate mobile apps privacy on a large scale. Enhancing the work presented before, crowdsourcing still presents a main component for gathering user's expectation related to the privacy behaviour of apps. The analysis of the past research lead to the following research questions:

RQ-1: What are people's privacy expectations of mobile apps?
RQ-2: Do people have correct mental models of mobile apps resource access behaviour?
RQ-3: Are privacy concerns and trust correlated with people's expectations?

In [22], the authors studied the compliance of accessing permissions by installed apps with regard to the users' expectation. To this end, they modified the Android OS to log whenever an installed app accessed a permission-protected resource and then gave modified smartphones to 36 participants who used them as their primary phones for one week. Afterwards, they showed various instances over the past week where apps had accessed certain types of data and asked whether those instances were expected, and whether they would have wanted to deny access. The results showed that 80% of the participants would have preferred to prevent at least one permission request, and overall, they stated a desire to block over a third of all requests. This is an important work that revealed the discrepancy between users' expectation and actual app behaviour. One of the most relevant outcomes from their work is identification of the need of transparency with regard to which app accesses which resources and at what frequency. A study from 2017 by Crager et al. [23] considered a different type of threat for users' privacy that comes from smartphones' sensors and other wearables. One

specific threat that they presented was from an advertising software developer kit (SDK), that used the smartphone's microphone to listen the near-ultrasonic sounds placed in the TV, radio and Web ads, which could be eventually used to infer the user's preferences. The results showed that users were only aware of the location tracking, and had not been considering the other three, namely Device-Fingerprinting, Keystroke-Monitoring and Acoustic Eavesdropping. As expected, users learning about the threats were immediately concerned about their privacy. The authors concluded that more efforts should be put into educating trivial (not experienced) users about the possible threats, but acknowledged the fact that the users would generally avoid using an app or a device if its security system affects usability.

Having included related work from 2011 to 2017, we conclude that although people are concerned, they are not in fact, fully aware how their data is being treated and how this affects their privacy. The part we shall be more concerned about is that the users, even after being alerted, tend not to change their behaviour (attitude) and instead try to rationalise using privacy-violating apps and willingly ignoring or accepting the possible risks. This behaviour, was coined in the literature as *privacy paradox* meaning that people's attitude toward privacy does not align with their actual behaviour [24,25]. This phenomenon is frequently assigned to psychological biases and heuristics that accompanies decision-making process. In the digital context the *privacy paradox* could be diminished by the reduction of information asymmetry. Currently, the end-users are not provided with a sufficient and understandable information about the data collection processes, unlike the service providers who have all the information about their data collection practice. Due to the lack of information, users are trapped in the *bounded rationality*, where the rational maximisation of benefits is restricted due to the limits of cognitive abilities [26].

Unlike the mentioned studies, we aim to increase the smartphone users awareness of privacy. By proposing a transparency tool called *Android Apps Behaviour Analyser (A3)* we analyse the behaviour of installed apps on the user's smartphone to identify privacy deviated activities. Out tool does not rely on the existing reviewed techniques for log analysis that require modification the OS (or root access). Additionally, we perform a user study to examine the users' privacy concern and expectation after revealing how much and to which level their personal information is accessed with/without their awareness. Hence, our remaining research questions are:

RQ-4: Is A3 tool capable of increasing mobile privacy awareness and altering privacy concerns?
RQ-5: What are people's reactions for the A3 tool and to the information it provides?

3 Technical Implementation: The A3 Tool

This section elaborates on the technical implementation followed in this paper to develop the *A3* tool including its respective components. Fig. 1 shows a high level

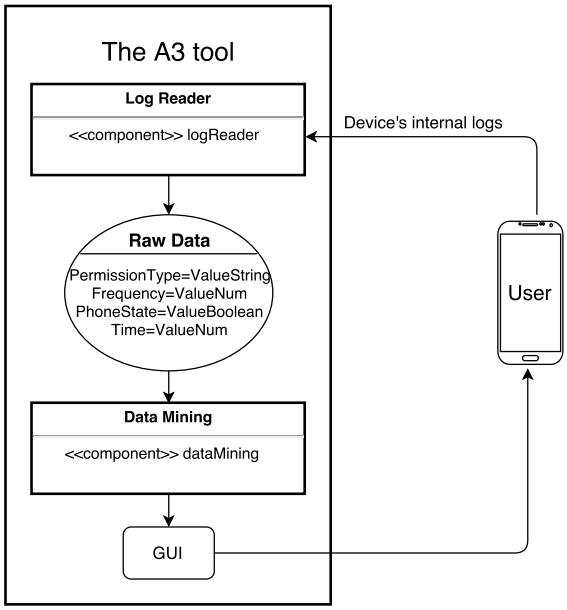

Fig. 1. A high level overview of the *A3* tool.

architecture of *A3*. As it can be seen, *A3* has several components. In principle, the log reader component is responsible to read device's logs, and accordingly, produce the raw data. These data are then sent to the data mining component which aims to analyse the apps' privacy behaviour. The results obtained from the data mining component are then sent to the user for further evaluation and decision.

3.1 Log Reader Component

Throughout the implementation phase, we consistently target three main goals. Firstly, *A3* must work without any need for root access to the OS. Secondly, there must not be any modification to the core of the OS. Lastly, it should be capable of being installed on the recent versions of Android. We implemented the log reader based on AppOps which is a privacy manager tool and introduced in Android 4.3. However, Google decided to make it hidden in later versions of Android and it is currently inaccessible, unless the device is rooted [27]. To the best of our knowledge, root access is only necessary to access the AppOps management system, e.g. to tell the system to deny access to one of the operations that is controlled by AppOps. We found that to view the AppOps logs, there is no need to root the device, and they are accessible to any app with debugging privileges [28, 29]. Generally, in order to collect the logs, a timer is sent to the `PermissionUsageLogger` service periodically. When it is received, the logger queries the AppOps service that is already running on the phone for a list of

apps that have used any of the operations we are interested in tracking. We then check through that list and for any app that has used an operation more recently than we have checked, we store the time at which that operation was used in our own internal log. These timestamps can then be counted to get a usage count.

3.2 Data Mining Component

This component is supposed to behaviourally analyse the installed apps by getting help from the results obtained from the log reader component. This is done according to a rule-based approach which is supposed to increase the functionality and flexibility of our data mining component. Consequently, we have defined a set of privacy deviated behaviour detection rules that are aimed to analyse the privacy behaviour of the users' installed apps. We initially defined a set of sensitive permissions (introduced by Android[4]) and we mainly analyse the accesses to these resources. For example, consider the device's screen is off and it is in the horizontal orientation (and the user does not talk on the phone, meaning that the `AUDIO` permission is not being used). In such situation, we assume that the user does not use the phone (e.g. the phone lies on the desk) and if one of the sensitive resources is accessed by a given installed app, we record this and report to the user about the detail of the access (date, time and reason together with a short explanation). Therefore, the users can transparently manage their resource accesses (due to space limitations, we refrained from explaining all the defined rules).

3.3 Graphical User Interface

The *A3* tool informs users of the potential misuses of their personal data. For this reason, we emphasise *how* the privacy indicators are shown to the user. Therefore, the Graphical User Interface (GUI) plays a crucial role in *A3*. The GUI offers the following functionality:

App selection In order to follow the principle of data minimisation [30], the users are given this option to choose the apps that they are interested to analyse their privacy behaviour, meaning that the users can freely choose which app(s) should be scanned (Fig. 2(a)).

Scan intervals We have given users the ability to decide about the desired scan intervals, meaning that they can determine the watchdog intervals at which the sensitive resources are scanned for any potential privacy invasive activity (Fig. 2(b)).

Permission restriction As Google has initiated a new permission manager system in Android 6.0 and later versions, we have embedded a direct access to this permission manager system to revoke/grant permissions for any app (Fig. 2(c)).

[4] https://developer.android.com/guide/topics/permissions/requesting.html

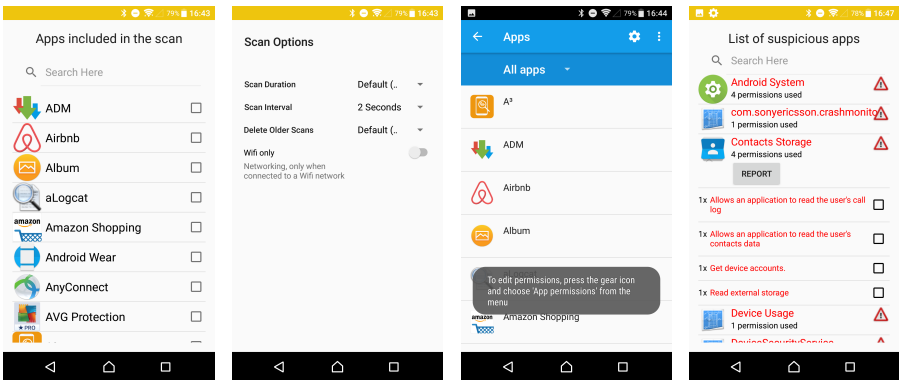

Fig. 2. *A3* user interface (a) app selection (b) scan intervals (c) permission restriction, and (d) behaviour analysis.

Behaviour analysis The users are able to check which personal resources (permissions) have been accessed by their installed apps. They can also observe the time and frequency of accesses. Accordingly, a synopsis of apps and resources accessed including the corresponding timestamps are communicated to the user. This also entailed to translate the technical terms of permissions defined by Android (e.g. `PHONE_STATE`, `COARSE_LOCATION`, etc.) to understandable definitions for the ordinary users (Fig. 2(d)).

4 The Design of the User Study

The user study comprises four main phases, including, recruitment, enter survey, a one week apps' behaviour analysis, and exit survey. In order to link enter and exit surveys, we supplied participants with an anonymous personal code. We asked participants about their privacy concerns, attitudes and expectations of the personal information that their smartphone would collect and transfer before and after using *A3*. The results gathered from this user study provide us with a sound foundation to compare the users expectations with actual results obtained from *A3*. This helps and supports users to judge to which extent their expectations match what the apps are doing in the reality. In the following, each phase is described in detail.

4.1 Recruitment

In total, 52 participants were recruited through placing an online recruitment advertisement on social networks (e.g. Facebook) within a three month time period (Nov 2017 to Jan 2018). In order to participate in the user study, the participants were asked to read and sign a consent form in which they stated

that they are over 18 years old and they own Android smartphones. To reduce potential biases, we requested for participants without advanced knowledge in computer science and IT related areas.

4.2 Enter Survey

In this phase, the participants were given certain questions about their: (1) privacy concern and (2) expectation of the smartphone apps behaviour. We tried to reuse the questions from [10, 18, 31, 32] and adapted them to our application domain. The majority of the survey used Likert [33] like item scales to measure the privacy concern and expectation of the participants in the area of smartphones. The scores ranged from one extreme attitude (not at all concerned) to another (extremely concerned). In the first set of questions, we collected data on participant demographics, privacy concern and expectation. In the demographics section, we asked participants to provide information on their demographic background, such as their age and gender. We then investigated participants' privacy concern when using a smartphone app in different scenarios such as when the information they shared was considered sensitive in general, or when an app accessed information that did not seem as relevant. Lastly, we collected data on participants' expectation of what information they believed had been accessed by different kinds of apps.

4.3 Apps Privacy Behaviour: A One Week Analysis

After the successful completion of the enter survey, the participants gave us the permission to install *A3* on their smartphones and they agreed to keep it running for one week. In order to make sure whether this one week time period is representative enough, we purchased ten Android smartphones and we installed the *A3* tool on them. We then let *A3* to run in the background for two weeks while it was scanning each individual phone (during this period, we never interacted with the devices, ensuring that they have sufficient battery level). We found that after almost one week, it is possible to observe a significant number of permission (resource) accesses by installed apps which would give us an indicator/understanding about the apps' behaviour. That is why we decided to choose the one week time slot. During the one-week interval, participants launched *A3* on their smartphones and performed their usual daily activities with their phones while the tool was scanning all the resource accesses by their installed apps. It is worth to mention that we did not collect any personal information and all the scan results remained on the users' phones (the analysis results were not transmitted to external parties, servers, etc.).

4.4 Exit Survey

At the end of the week, the participants returned to our lab. They were presented with the results of the analysis of their installed apps' behaviour and completed

Table 1: Participants demographics.

Demographic	Group	N	%
Age	18-24	16	30.8
	25-34	25	48.1
	35-44	7	13.5
	45 or older	4	7.7
Gender	Female	22	42.3
	Male	30	57.7
Education	High school	4	7.7
	Some college	4	7.7
	Bachelors degree	30	57.7
	Masters degree or higher	14	26.9
IT experience	Not at all	21	40.4
	Trivial	20	38.5
	Moderate	9	17.3
	A lot	2	3.8

the exit survey. We asked the participants to go through the results of the scans to see how their personal resources have been treated by their installed apps during the one week period. The questions in the exit survey examined how participants' expectation changed as a result of using *A3*, e.g. whether they changed their privacy attitude, do they have the intention/willingness to change their behaviour, what do they think about *A3*, whether its results are informative, annoying, expected, etc. Finally, each participant was compensated by a €15 Amazon voucher.

5 Results

5.1 General Exploration over the Data

Among 52 study participants, the majority (48.1%) were between 25-34 years old. The sample was almost equally distributed among two genders, females (42.3%) and males (57.7%). Most of the respondents held higher education, either bachelor's (57.7%) or master's degree and higher (26.6%). The detailed demographics are presented in Table 1.

Only three (5.7%) participants admitted that they read privacy policy before installing the new smartphone app, while 17 (32.7%) said they never read it, 23 (44.2%) said they read it rarely, and nine (17.3%) sometimes. The majority of respondents expressed their lack of knowledge about privacy in general ($N = 31$, 59.6%). Most of them were certain ($N = 23$, 32.7%) or not sure ($N = 16$, 30.8%) whether they have a basic knowledge about technical terms of privacy and security.

The participants admitted that they prefer social media and convenience to privacy and security. 16 (30.8%) said it is very true and 16 (30.8%) said rather

true. Additionally, 33 (63.5%) participants confessed that they actively use social media.

Regardless, most participants stated that they feel motivated, and spend considerable time trying to protect their online privacy ($N = 32$, 61.5%). 29 (55.8%) respondents did not feel confident that somebody could track or monitor their online activities, and 15 (28.8%) were not sure how they feel about it.

5.2 User Expectation

In the enter survey we asked participants about their expectations of apps behaviour (**RQ-1**). First, we wanted to know how likely they think the app which they did not create an account for, will have access to sensitive information (i.e. location, contacts, etc.). The majority of participants said that it is not likely ($N = 22$, 42.3%) or only slightly likely ($N = 12$, 23.1%). The small percentage of respondents thought it is moderately ($N = 10$, 19.2%), or very and extremely likely ($N = 8$, 15.3%). Additionally, we asked to what extent the respondents agree with the following statement *Smartphone apps are only accessing resources and permissions which are related to their functionality (e.g. navigation apps need to have access to your location etc.)*. In total 20 participants strongly or somewhat agreed with the statement (38.4%), and 13 (25%) were neutral about it.

We wanted to examine whether participants would like to know more about the data collection and processing of smartphone apps. First, we asked if they would like to know what personal information is accessed by apps installed on their smartphones. The majority of participants strongly agreed ($N = 36$, 69.2%) or somewhat agreed ($N = 10$, 19.2%) with such statement. Additionally, we asked whether they would like to know how their personal information is used by apps installed on their phones. Once again, the participants even strongly agreed ($N = 39$, 75%) or somewhat agreed ($N = 9$, 17.3%) that they wish to know it.

5.3 App Resource Access Behaviour

We were interested to identify whether participants have the correct mental model for the frequency of access to the phone resources of certain app types (**RQ-2**). Therefore, in the enter survey we asked participants whether they have a social network, messaging and navigation app installed (most common sensible app categories to ordinary users), and if so, how many times such app is accessing their phone's location, storage, contacts, accounts, phone number, audio, calendar, camera and SMS/MMS. To see whether the assumptions were close to reality, in the exit survey we asked respondents to provide the access information from the *A3* tool, collected over the week.

In general, respondents underestimated the frequency of resource access by different apps. Among the respondents who had social network app on their phones ($N = 34$), 48.1% underestimated the location access, 59.6% storage, 30.8% contacts while 38.8% overestimated camera access. Similarly, the owners

of messaging apps ($N = 46$) underestimated the numbers of access to location ($N = 20$, 30.8%), storage ($N = 43$, 88.5%), contacts ($N = 34$, 65.4%), accounts ($N = 33$, 63.5%), audio ($N = 28$, 53.8%), camera ($N = 21$, 40.4%). Lastly, the respondents highly underestimated the navigation apps resource access, such as location ($N = 41$, 78.7%) and storage ($N = 44$, 84.6%). We found that the real frequencies of apps accessing various resources vary, and where really high, some of them reaching over 40000 times per day.

5.4 Privacy Concern Aspects in Smartphone Apps

General Privacy Concerns and Trust We developed a Likert scale [33] to investigate privacy concerns and online trust. We checked the reliability, and Cronbach α was .848 for the five *trust* items, and .754 for the five *privacy concerns* items. The Cronbach alpha is a reliability test that should be applied to check whether the scale is consistent, and whether it measures the desired attitude. It is based on the calculation of the average value of the reliability coefficients of all available items when divided into two half-tests [34].

We applied Spearman test for correlations to investigate whether there are relationships between privacy concerns, trust and expectations (**RQ-3**). The Spearman correlation was used because the data did not meet the assumptions of parametric tests. Spearman correlation is used on the ranked data, and it measures the strength of the relationship between two variables [35]. We found significant correlations between *trust* and the role of an app reputation when deciding upon personal information disclosure ($r_s = .35$, $p < .05$). There was a positive correlation between *trust* and a belief that an app accesses only resources related to its functionality ($r_s = .49$, $p < .001$). Additionally, we found a negative correlation between *trust* and refusal of providing personal data to smartphone apps ($r_s = -.41$, $p < .05$), apps' access to sensitive information ($r_s = -.30$, $p < .05$) and the restrictions of applications' permissions ($r_s = -.40$, $p < .05$).

Further, we found a significant correlation between *privacy concerns* and willingness to uninstall the app, if it violates users' privacy ($r_s = .38$, $p < .05$). Lastly, there was a correlation between concerns and fear about the safety of information ($r_s = .30$, $p < .05$).

We used Spearman test for correlations to examine whether people with higher levels of *privacy concerns* rank higher the importance of clear information about app's access to different types of personal information (when deciding on app's download or usage). We identified positive correlations between privacy concerns and importance of information about access to the phone's location, storage, contacts, accounts, audio, and camera (Table 2).

Privacy Issues in Smartphone Apps One of the research goals was to investigate whether the *A3* tool is capable of increasing smartphone users' privacy awareness (**RQ-4**). To examine this we used repetitive measures, pre- and post questionnaires asking participants about their privacy concerns in the context of smart-phone apps. We applied Wilcoxon test to measure whether the participants' level of privacy concern changed after using *A3*. We used Wilcoxon

Table 2: Spearman correlations: privacy concerns and importance of clear information about the apps access to different types of personal information.

Information type	Correlation	Sig. (2-tailed)
Location	.494	.000
Storage	.335	.015
Contacts	.362	.008
Accounts	.522	.000
Audio	.386	.005
Camera	.508	.000

test because we it is suitable for ordinal, ranked data. This test enables a direct comparison in related design studies, between participant's scores in two conditions [36].

The test indicated that in the exit survey, participants scored significantly higher on concerns about personal data being leaked or transferred to third parties ($Z = -5.106, p < .001$). Similarly their concerns were significantly higher about data falsification ($Z = -4.088$, $p < .001$), online bullying and flaming ($Z = -3.7006$, $p < .001$), receiving spam emails ($Z = -5.056, p < .001$), and receiving behavioural adds ($Z = -4.080, p < .001$). Further, after a week of using *A3* participants were more worried about government surveillance ($Z = -4.375$, $p < .001$) and about apps accessing irrelevant information ($Z = 5.442, p < .001$). However, there was no significant difference in before and after scores regarding the level of concern about their credit card being used by others.

5.5 Reaction to the Transparency Tool

Overall, we were interested in how the participants react to the A3 tool, and to the information it has provided (**RQ-5**). After using the *A3* tool for a week, the majority of respondents were surprised to learn how often apps access their personal resources ($N = 46$, 88.5%). The respondents found information provided by *A3* shocking ($N = 40$, 76.9%) but informative ($N = 36$, 69.3%). The participants realised that some apps access permissions that are not related to their functionality ($N = 49$, 94.3%), and they were shocked about it ($N = 46$, 88.4%). In regards of privacy intentions and concerns, participants expressed the willingness to restrict apps permissions in the future ($N = 46$, 88.5%), as well as uninstalling some of the apps that they find privacy invasive ($N = 40$, 86.9%). The majority ($N = 46$, 88.5%) found themselves more worried about privacy than before using *A3*, and they intend to report privacy invasive behaviours ($N = 32$, 61.6%), e.g. in the form of user comment on the Google Play Store to increase the privacy awareness of other users. Similarly, they expressed a willingness to read privacy policies before installing the app ($N = 36$, 69.3%). Lastly, the respondents admitted they would like to have tool like *A3* earlier ($N = 47$, 90.4%) and if possible wish to use it to monitor their smartphone apps behaviour ($N = 43$, 82.7%).

Table 3: Spearman correlations: privacy concerns and trust with information sensitivity.

	Sensitive information	Correlation	Sig.(2-tailed)
Privacy Concerns	Location	.286	.040
	Storage	.417	.002
	Accounts	.277	.047
	Audio	.326	.018
	Calendar	.327	.018
Trust	Contacts	-.277	.047
	Calendar	-.346	.012
	SMS/MMS	-.276	.047

5.6 Additional Findings

Privacy Sensitivity Degree of Different Smartphone Resources We asked respondents about the sensitivity of different types of information, on a scale from *Not at all sensitive* to *Extremely sensitive*. The participants perceived as extremely sensitive storage information (photos & videos)(N = 20, 38.5%), audio (N = 15, 28.5%), camera (N = 17, 32.7%). They perceived as a not at all sensitive calendar information (N = 16, 30.8%) and SMS/MMS (N = 13, 25%). The other information types were scored as moderately (accounts on your phone, phone number) or slightly (location, contacts) sensitive.

The Spearman correlation tests identified significant positive correlations between the information sensitivity and privacy concerns. There was a weak correlation between concerns and sensitivity of location and accounts. Additionally, sensitive information about the storage, audio and calendar was correlated with concerns. Further, we found that there is a significant negative correlation between trust and sensitivity level of contacts, calendar and SMS/MMS information. The results of correlation analysis are presented in Table 3.

5.7 Discussion

Our findings confirm that *A3* is able to affect the way by which people are concerned about their privacy. Although the majority of the participants (65.4%) said it is not likely or slightly likely that an app which they did not create an account for, will have an access to sensitive resources, the participants realised it is incorrect. They reported a higher number of apps that were not being used by them during the one week analysis, but still they were accessing users' personal resources in a very aggressive manner (without any user interaction, e.g. account creation, etc.). Further, 38.4% of the participants believed that smartphone apps only access resources relevant to their functionality (e.g. a weather forecasting app requires access to location). However, we discovered that some apps (e.g. health & fitness, navigation, etc.) that do not need to excessively request or access privacy sensitive information, are doing so without users' knowledge.

Overall, the information provided by *A3* raised the participants' privacy awareness after a trial period. This indicates that the reduction of information asymmetry by providing users with information about the apps resource access, may help to overcome or at least reduce the *privacy paradox*. However, this requires further investigation in different experimental settings enabling examination of causal relationship between the attitude and behaviour prior and after using the *A3* tool. Additionally, our results demonstrated that users have an inaccurate mental model of apps' resource access behaviour, and they mostly underestimated the frequency of permission accesses by their installed apps. However, the participants expressed willingness to change their attitude and behavior after using the tool. This willingness to change suggests that the tool such as *A3* could adjust users mental models, raising privacy awareness and enabling informed privacy decision-making.

5.8 Limitations

The scope of this paper comprises Android OS. Regardless of the choice of the research area, currently the *A3* tool cannot be applied to other smartphone platforms (e.g. iOS). Another limitation is the low number of participants (52 people) due to the complexity of the study. This happened due to several reasons. Firstly, *A3* is solely executable on Android devices, correspondingly, we missed lots of participants who showed interest but they were not technically qualified to participate in the study (e.g. iOS users). Secondly, since *A3* is not publicly available on the Google Play Store, several interested people expressed that they do not feel comfortable to install an app from unknown sources on their phones. Further, we tried our best to keep the study safe from any biases (e.g. to not focus on privacy experts). Unfortunately, in such studies, it is challenging to have a diverse type of participants which would further enhance the validity of our analysis.

6 Conclusion

In this paper, we studied the smartphone users' privacy awareness by conducting a user study based on an implemented privacy enhancing tool (*A3*). We examined the applicability of such tool with the real users and investigated the users' reaction to *A3*. Thus, we performed a user study comprising of 52 participants and we analysed their privacy concern and expectation before and after using the *A3* tool. The results clearly showed that users' privacy concern and expectation changed after using *A3*. We identified that users' privacy awareness increased due to the implication of *A3*. Moreover, we observed that users mostly have poor knowledge of how their installed apps treat their personal sensitive resources. Additionally, we found that there is a gap between what smartphone users perceive about privacy and what is happening in the reality by their installed apps. Study participants were shocked once they understood how their apps are accessing their resources without their knowledge, especially

when accessing resources that are not necessary for the appropriate functionality of an app. As a result, we believe that the smartphone users need such privacy enhancing tool to better protect their privacy and to make informed privacy decisions. Although the results showed the changed perceptions of privacy issues that might be due to the use of *A3*, for the future work we plan to implement an explanatory study investigating the role of *A3* tool in the causal relationship of privacy attitude-behaviour change. This will enable us to contrast the control group with the experimental group for a more confident comparative analysis.

References

1. P. Gilbert, B. G. Chun, L. Cox and J. Jung, "Automating privacy testing of smartphone applications," Technical Report CS-2011-02, Duke University (2011)
2. E. Raad and R. Chbeir, "Privacy in online social networks," Security and Privacy Preserving in Social Networks, Springer-Verlag Wien, 3–45 (2013)
3. B. Razeghi and S. Voloshynovskiy, "Privacy-Preserving outsourced media search using secure sparse ternary codes," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, Canada, 1–5 (2018)
4. B. Razeghi, S. Voloshynovskiy, D. Kostadinov and O. Taran "Privacy preserving identification using sparse approximation with ambiguization," in *Proceedings of IEEE International Workshop on Information Forensics and Security (WIFS)*, Rennes, France, 1–6 (2017)
5. "Number of apps available in leading app stores," accessed April 5th, 2018, https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/
6. "Number of mobile app downloads worldwide in 2016, 2017 and 2021," accessed April 5th, 2018, https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/
7. "eMarketer unveils new estimates for mobile app usage," accessed April 5th, 2018, https://www.emarketer.com/Article/eMarketer-Unveils-New-Estimates-Mobile-App-Usage/1015611
8. "Report: Smartphone owners are using 9 apps per day, 30 per month," accessed April 5th, 2018, https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month/
9. "More time on Internet through smartphones than PCs," accessed April 5th, 2018, https://marketingland.com/nielsen-time-accessing-internet-smartphones-pcs-73683
10. J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing," in *Proceedings of ACM Conference on Ubiquitous Computing (UbiComp'12)*, Pittsburgh, Pennsylvania, USA, 501–510 (2012)
11. A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the 8th ACM Symposium on Usable Privacy and Security (SOUPS'12)*, New York, NY, USA, 1–3 (2012)
12. A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns," in *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'12)*, New York, NY, USA, 33–44 (2012)

13. D. J. Solove, "Nothing to Hide: The False Tradeoff between Privacy and Security," Yale University Press, (2011)
14. "Your apps are watching you," accessed April 5th, 2018, https://www.wsj.com/articles/SB10001424052748704694004576020083703574602
15. "Appthority exposes security and privacy risk behind top 400 mobile apps," accessed April 5th, 2018, https://www.appthority.com/company/press/press-releases/appthority-exposes-security-and-privacy-risks-behind-top-400-mobile-apps/
16. P. H. Chia, Y. Yamamoto, and N. Asokan, "Is this app safe?: a large scale study on application permissions and risk signals," in *Proceedings of the 21st International Conference on World Wide Web*, Lyon, France, 311–320 (2012)
17. P. G. Kelley, M. Benisch, L. F. Cranor, and N. Sadeh, "When are users comfortable sharing locations with advertisers?," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Vancouver, BC, Canada, 2449–2452 (2011)
18. E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the 8th Symposium on Usable Privacy and Security*, Washington, D.C., USA, Article No. 1 (2012)
19. A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns," in *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, Raleigh, North Carolina, USA, 33–44 (2012)
20. S. Amini, "Analyzing mobile app privacy using computation and crowdsourcing," in *Proceedings of the ACM Conference on Ubiquitous Computing*, Ph.D. Dissertation (2014)
21. S. Amini, J. Lin, J. I. Hong, J. Lindqvist, and J. Zhang, "Mobile application evaluation using automation and crowdsourcing," in *Proceedings of the Workshop on Privacy Enhancing Tools* (2013)
22. P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov, "Android permissions remystified: A field study on contextual integrity," in *Proceedings of the 24th USENIX Security Symposium*, Washington, D.C., USA, 499–514 (2015)
23. K. Crager, A. Maiti, M. Jadliwala, and J. He, "Information leakage through mobile motion sensors: User awareness and concerns," in *Proceedings of the 2nd European Workshop on Usable Security*, Paris, France, 1–15 (2017)
24. B. Brown, "Studying the Internet experience," *HP Laboratories Technical Report HPL*, http://shiftleft.com/mirrors/www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf (2001)
25. P. A. Norberg, D. R. Horne and D. A. Horne, "The privacy paradox : Personal information disclosure intentions versus behaviors, " The Journal of Consumer Affairs, vol. 41, no. 1, 100—126 (2007)
26. A. Acquisti, C. R. Taylor and L. Wagman, "The economics of privacy," Journal of Economic Literature, vol. 54, no. 2, 442-–492 (2016)
27. "Google removes vital privacy feature from Android, claiming its release was accidental," accessed July 17, 2016, https://www.eff.org/deeplinks/2013/12/google-removes-vital-privacy- features-android-shortly-after-adding-them/
28. M. Hatamian and J. Serna-Olvera, "Beacon alarming: Informed decision-making supporter and privacy risk analyser in Smartphone applications," in *Proceedings of the IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 468–471 (2017)

29. M. Hatamian, J. Serna, K. Rannenberg and B. Igler, "FAIR: Fuzzy alarming index rule for privacy analysis in smartphone apps," in *Proceedings of the 14th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2017)*, Lyon, France, 3–18 (2017)
30. Article 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, vol. 59 (2016)
31. N. Aldhafferi, C. Watson, and A. S. M Sajeev, "Personal information privacy settings of online social networks and their suitability for mobile internet devices," International Journal of Security, Privacy and Trust Management, vol. 2, no. 2, 1–17 (2013)
32. A. Rao, F. Schaub, N. Sadeh, A. Acquisti, and R. Kang, "Expecting the unexpected: Understanding mismatched privacy expectations online," in *Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS)*, Denver, CO, USA, 77–96 (2016)
33. R. Likert, "A technique for the measurement of attitudes," Archives of Psychology, vol. 22, 5–55 (1932)
34. J. A. Gliem and R. R. Gliem, "Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for likert-type scales," in *Proceedings of Midwest Research to Practice Conference in Adult, Continuing, and Community Education*, Columbus, Ohio, USA, 82–88 (2003)
35. A. Field, J. Miles and Z. Field, "Discovering statistics using SPSS," Sage Publications Ltd (2013)
36. J. Greene and M. D'Oliveira, "Learning to use statistical tests in psychology," Open University Press (2005)