Does This App Respect My Privacy? Design and Evaluation of Information Materials Supporting Privacy-Related Decisions of Smartphone Users

Oksana Kulyk*, Paul Gerber†, Karola Marky‡, Christopher Beckmann* and Melanie Volkamer*
*Karlsruhe Institute of Technology
Email: name.surname@kit.edu
†Institute of Psychology
Technische Universität Darmstadt
Email: gerber@psychologie.tu-darmstadt.de
‡Telecooperation Lab
Technische Universität Darmstadt
Email: marky@tk.tu-darmstadt.de

***Abstract*—Over the years, the wide-spread usage of smartphones leads to large amounts of personal data being stored by them. These data, in turn, can be accessed by the apps installed on the smartphones, and potentially misused, jeopardizing the privacy of smartphone users. While the app stores provide indicators that allow an estimation of the privacy risks of individual apps, these indicators have repeatedly been shown as too confusing for the lay users without technical expertise. We have developed an information flyer with the goal of providing decision support for these users and enabling them make more informed decisions regarding their privacy upon choosing and installing smartphone apps. Our flyer is based on previous research in mental models of smartphone privacy and security and includes heuristics for choosing privacy-friendlier apps used by IT-security experts. It also addresses common misconceptions of users regarding smartphones. The flyer was evaluated in a user study. The results of the study show, that the users who read the flyer tend to take privacy-relevant factors into account by relying on the heuristics in the flyer more often. Hence, the flyer succeeds in supporting users in making more informed privacy-related decisions.**

I. Introduction

Mobile devices, in particular, smartphones have gained particular prominence in people's lives and are used on a daily basis for a variety of tasks. As a result, these devices accumulate large amounts of personal data, such as contacts, pictures, or information about the user's location. Correspondingly, these data can be accessed by smartphone apps that are installed by the users. Misuse of such data by a malicious app provider can pose a serious threat to the users' privacy, defined as the possibility of controlling the circumstances and conditions under which personal information is collected and processed by third parties [7], [24].

Yet, research has shown that users often fail to consider necessary precaution measures to protect their privacy (e.g., [3], [28]). A possible reason for the neglection of privacy friendly behavior is that users often do not take privacy into account when making decisions in their day-to-day smartphone usage. This is partially due to users being unaware of privacy risks or underestimating them, but also because privacy is not the primary task of the users, as opposed to main functionality of the apps, such as sending messages or checking the weather report [9].

On the other hand, even if the users are willing to protect their privacy, they often lack the knowledge on how to do so. While there are indicators like permission warnings, previous research has shown that these are often deemed to be confusing for the users [12]. Furthermore, a number of prevalent misconceptions, such as the belief that all apps in the official stores (Apple Store or Play Store) do not pose any risk [18] often prevent users from taking proper protection measures. The research in usable security and privacy therefore recognizes the need to consider the existing mental models and knowledge of the end users for developing measures for supporting and encouraging security and privacy friendly behaviour [26].

In an attempt to support users in decision making regarding smartphone apps, a study by Kulyk *et al.* [14] interviewed IT-security experts about how they choose and install smartphone apps. As the experts were expected to possess the necessary knowledge and awareness regarding privacy and to attempt to optimize their day-to-day practices, the authors used the results from their interviews to derive a set of heuristics. These heuristics were designed to support users in making informed privacy-related decisions regarding the management of apps on their smartphone. The effectiveness of the derived heuristics has not been evaluated yet.

In this work, we aim to develop a concept for information materials, designed to support informed privacy-related decisions for smartphone end users. Therefore, we rely on the heuristics developed by *Kulyk et al.* [14] that are presented to the user. In addition to the heuristics, we furthermore aim to raise awareness among the users and motivate them for

Workshop on Usable Security (USEC) 2019
24 February 2019, San Diego, CA, USA
ISBN 1-891562-57-6
https://dx.doi.org/10.14722/usec.2019.23029
www.ndss-symposium.org

considering their privacy as a decision criterion in choosing smartphone apps. For this, we address common misconceptions among smartphone users regarding their privacy which we derived from a literature review. The developed concept has furthermore been implemented as an information flyer and evaluated in a user study with 38 participants. The results of our study show, that the flyer succeeds in supporting informed decisions of smartphone users by leading them to consider privacy to a larger extent in their decisions.

The remainder of this paper is structured as follows. We describe our literature review, explain the resulting misconceptions of smartphone users and summarize the heuristics from [14] in Section II. We describe the contents of the flyer incorporating the heuristics and addressed misconceptions in Section III. Section IV describes our user study conducted to evaluate the developed flyer, and the results of the evaluation are provided in Section V. We discuss the results in Section VI, followed an overview of related work in Section VII, and conclude the paper in Section VIII.

II. Background

In this section we describe the background which we relied upon in the development of the content for our concept.

A. Smartphone Privacy Misconceptions

As our goal was to address the common misconceptions that prevent the users from protecting their smartphone privacy, we conducted a literature research[1] in order to find out what these misconceptions are. In this, we searched the scientific literature databases *SpringerLink*, *ACM*, *IEEE*, *Scopus* and *Science Direct* using the following search terms: ”smartphone misconception”, ”smartphone misunderstanding”, ”smartphone misperception”, ”smartphone flawed perception”, ”smartphone flawed understanding”[2]. We limited our search to peer-reviewed articles in English language, the full text of which were available via our institution. Among the results, we looked for the publications that conducted qualitative studies on the security and privacy related misconceptions for smartphones. We omitted the publications that either provided the misconceptions very specific to a particular OS version (such as a misunderstanding of the explanation text of an Android permission). We furthermore omitted misconceptions that, while relying on an incorrect mental model of the users, do not lead to insecure behaviour. For the remaining publications we conducted a forward reference search using the same search terms.

The literature review resulted in nine publications [1], [2], [5], [12], [17], [18], [21], [25], [27]. The misconceptions found in these publications can be summarized as follows:

- ”I have nothing to hide”: the users’ belief that they would not be harmed by potential privacy violations.
- ”I am too unimportant”: belief that only prominent people such as politicians or CEOs can become targets of attacks on their privacy
- ”If my smartphone is secured, my privacy is ensured as well”: belief that the privacy can be violated only via attacks and malware apps.
- ”Only the data that is input explicitly can be leaked”: belief that the data can be collected only if the users input it in an app themselves.
- ”If the company is trustworthy, then it is safe to provide my data to them”: belief that trustworthy companies always manage to keep their customer’s data secure.
- ”There is nothing I can do against it”: belief that the users are powerless to protect their privacy against attackers and companies that collect their data.

B. Privacy-Friendly App Choice Heuristics

In order to support the users who want to take measures and protect the privacy on their smartphones, we chose to provide a list of heuristics that the users can apply when installing and using smartphone apps. Therefore, we relied on the previous work by Kulyk *et al.* [14] that interviewed IT-security experts with the goal of eliciting heuristics that these experts use. These heuristics are classified into the following four categories:

1) **Permission-related:** These heuristics relate to the permissions requested by the app, such as considering whether the permissions are reasonable given the app’s functionality.
2) **Developer-related:**These heuristics relate to the developers of the app, such as reviewing the website of the developers to evaluate their trustworthiness.
3) **Socially-related:**These heuristics relate to the feedback of other users for the app, such as searching the app’s reviews for mentioned privacy issues.
4) **Avoidance techniques:**These heuristics aim to minimize the exposure of data to apps, such as avoiding the storage of data that is particularly sensitive on a smartphone.

III. Flyer

In this section we describe our developed concept in a form of an information flyer[3]. The flyer has been developed via multiple iterative feedback sessions in order to incorporate feedback from potential users early during the design process. The flyer is structured into the two parts *misconceptions* and *heuristics*. We describe both of the parts in more details below.

A. Part I: Misconceptions

The first part is structured as an FAQ and addresses the common misconceptions that prevent the users from protecting their smartphone privacy. The purpose of this part is to make the users aware of the possibility of privacy violations on their smartphone and to motivate them to take protection measures against such violations. To develop this part we relied upon misconceptions found via a literature review described in Section II-A. For each misconception, we provided a response as follows[4]:

[1] The research was conducted in August 2017.

[2] Note, the search terms included only ”smartphone” and not the ”smart phone” word form.

[3] The flyer is available under https://secuso.org/smartphone-privacy-flyer, including the version used our study.

[4] Translated from German.

1) "I have nothing to hide": Even if you do nothing illegal, collecting your data has disadvantages. For instance, the data could be used by hackers to learn more about you. This knowledge could be used for a targeted attack (so-called Spear Phishing) against you by sending e-mails with personal information. Furthermore, the more someone know about you, the easier it gets to influence your buying behavior or election decisions. Additionally, keep in mind the exact knowledge about your current whereabouts in criminal hands (such as burglars) can pose a serious threat.

2) "I am too unimportant": It is very easy to collect data in a large scale, especially as many things are shared publicly. Even if you consider it unlikely that you could be "interesting", your data (e.g. who you call at what time) are collected.

3) "If my smartphone is secured, my privacy is ensured as well": Privacy and security of a device do not necessarily have something to do with each other. Especially because a lot of your data is quite often collected by companies from apps and advertising networks and resold.

4) "Apps from app stores are secure by default": While avoiding apps from inofficial stores is a good protection strategy, the official stores are not immune to malicious software. The stores contain millions of apps and these are not all individually tested by hand. Furthermore, apps that are not technically malware can still collect and share your private information.

5) "Only the data that is input explicitly can be leaked": Because of the way smartphones work, apps have often not only access to direct input, but also on personal data stored on the smartphone (e.g., images). This can be done without your knowledge in the background.

6) "If the company is trustworthy, then it is safe to provide my data to them": Even trustworthy companies can become the victims of hacker attacks. You should be careful and consider what data is really needed for the features, even if you trust the company.

7) "There is nothing I can do against it": Although some services and apps need access to private data for their basic functions, there are many privacy-friendly alternatives. What you can do against it is written on the following pages of this flyer.

B. Part II: Heuristics

The second part of the flyer is based on the heuristics by Kulyk *et al.* that we describe in Section II-B. The users can apply these heuristics during the installation or usage of smartphone apps in order to minimize the risks of privacy violations by these apps. Whenever possible we provided information where to find the relevant information (e.g., information regarding permissions required by an app) in the Play Store.

We transformed the four heuristic categories, which in total contain thirteen heuristics, into ten guidelines for our flyer. Note, the heuristics by Kulyk *et al.* were derived from the practices of IT-security experts, therefore some of them include recommendations that rely on some sort of additional technical expertise. Since our flyer is designed for lay users, we modified the heuristics accordingly. We describe the resulting guidelines in more detail below.

1) Permissions: The user is advised to check the reasonability of permissions. If a permission does not match the app's functionality, the user is advised either not to install the app or not grant to permission. Furthermore, it is described where the user can gather information of an app's required permissions in the Play Store. The permission-related heuristics by Kulyk *et al.* furthermore allows accepting a permission in case the data sharing can be minimized with other means, for example, by using additional software. We did not transform this info a guideline since this requires expert knowledge, but our flyer targets ordinary users.

2) App functionality: In this part of the flyer, the user is advised to check the functionality of an app. The app should not contain functionality that is superfluous for the user. The more superfluous functionality an app has, the more likely it is that the app requires non-reasonable permissions.

3) Number of downloads: The user is advised to check the number of downloads of an app and to prefer those with a big user basis. Furthermore, this heuristic contains a description where to find the number of downloads in the Play Store.

4) Reviews of other users: The reviews of other users should be read carefully. Especially negative reviews or those mentioning privacy issues of an app should be taken into account when making the decision whether to install an app. A description where to find the number of downloads in the Play Store is also given to the user.

5) On-going development: On-going development meaning the last update of an app is an indicator for potential privacy issues. If an update lies long in the past, the developer might not have patched security loopholes. A description where to find the last update is given to the user.

6) Developer: The user is advised to check the app's developer. To gain information about the developer, the user can visit the developer's website. The following aspects indicate the trustworthiness of a developer:

- The developer offers many apps to a large user base.
- The developer is from a country with legal regulations regarding data privacy.
- The developer is a large company with a good reputation.
- The developer provides a privacy policy.

The developer-related heuristics by Kulyk *et al.* contain "contact to the developer" meaning that the user can seek direct contact to the developer before making their decision about app installation. Due to the potential complexity of the process involved, we did not include this heuristic into our flyer.

7) Other apps of the developer: The user is advised to look for other apps by the same developer in the Play Store. The previously mentioned heuristics should also be considered for those other apps.

8) Media reports about the app or its developer: News and media reports about the app and its developer can help the users in making the decision whether to install the app. Users are guided to look for privacy as well as security-related reports.

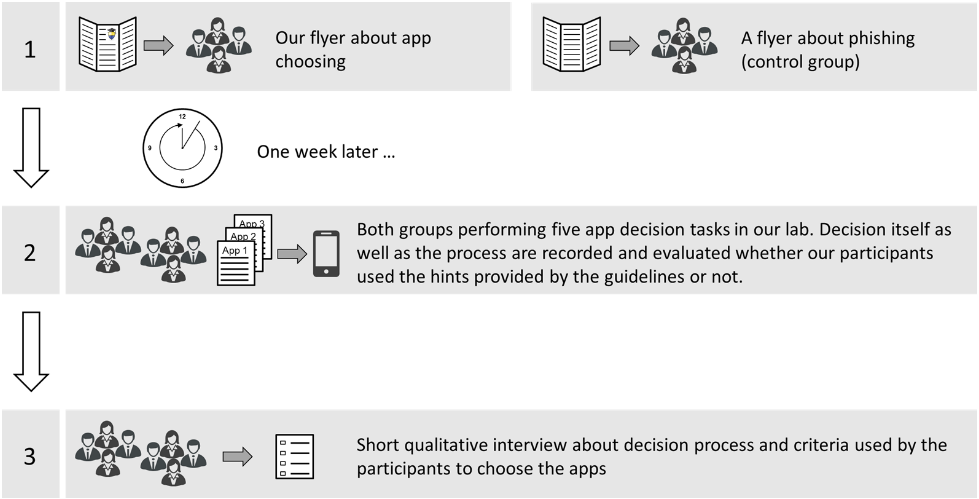
1
Our flyer about app choosing
A flyer about phishing (control group)
One week later ...
2
App 3
App 2
App 1
Both groups performing five app decision tasks in our lab. Decision itself as well as the process are recorded and evaluated whether our participants used the hints provided by the guidelines or not.
3
Short qualitative interview about decision process and criteria used by the participants to choose the apps

Fig. 1. Graphical overview of the study design.

9) Deinstallation of unused apps: Besides the guidelines about information that user should consider before installing an app, the flyer contains the advise to regularly check apps that are installed on the device. If apps are not required any longer, the user is advised to uninstall them, because uninstalled apps can no longer lead to data leakage. Furthermore, the flyer contains information on how to deinstall an Android app.

10) Transfer of sensitive data to other devices: Finally, the user is advised to transfer privacy sensitive data (e.g., pictures) to another device. By doing so, privileged apps have access to less privacy-sensitive data.

The avoidance techniques by Kulyk *et al.* contain *"avoid negative vibes"* meaning that experts use their expert knowledge to make a judgment. We did not include this heuristic into our flyer, because the flyer does not target expert users.

IV. User Study

The study design is briefly presented in Figure 1 and described in more detail below. Afterwards, the store app that we used for our study is presented in detail as well as the tasks we asked from the participants. Subsequently, the sample is described in more detail and finally the hypotheses to be tested are presented.

A. Study Design

All participants were randomly drawn to either the trial group or the control group. Each participant was sent a flyer by e-mail seven days before the test date. In the case of the experimental group, this was our flyer with heuristics on app selection (see Section III), in the case of the control group a flyer on phishing attacks and how to protect yourself against them. The mentioned goal of the study was to evaluate a new app. The experiment itself took place in a laboratory of the Institute of Psychology at the university and lasted between 20 and 30 minutes.

In the laboratory, all participants received a short oral instruction on the test procedure. This entailed that they were to select a total of five different apps from four different alternatives. Throughout the study the participants did not use their own smartphones, but were provided with a lab device. In each case, they should use the store app that we have programmed (see Section IV-B), which is to be evaluated. No more detailed evaluation targets were mentioned. Furthermore, the participants were informed that the contents of the screen will be recorded during the experiment so that a later evaluation of the user interaction can be carried out. Afterwards, each participant was given a written instruction with the type of app to be searched for and the functional requirements. The order of the five different app categories was randomly determined for each participant. As soon as the participant was satisfied with his or her decision, he or she informed the investigator and was handed over the next of the five tasks.

After all five tasks were completed, the screen recording was finished. Participants were then asked about each decision. First of all, the criteria considered were asked for each individual app decision. Subsequently, the individual criteria were named on the basis of the heuristics (see Section III-B) and asked whether they were taken into account for the decisions. These included the following: (1) the developer, (2) requested app permissions, (3) if functionality equals the instructions, (4) number of downloads, (5) user reviews, (6) the app rating, (7) the date of the last update.

Finally, each participant was asked if and when he or she read the flyer. In addition, he or she was asked to briefly summarize the contents of the flyer. Afterwards, the gender, age, the Android version used on the own device, and the student's course of study or profession were recorded.

B. Study App

The participants used a lab device with a mock Play Store app for choosing and installing apps within our study. The mock Play Store was specifically designed and implemented for the purpose of the study. Our mock Play Store app mimics the design of Google Play Store, such that the participants had the same user experience choosing and installing apps as they have on their private devices. To make sure that participants do not choose apps that they previously knew, all apps and their icons in the mock Play Store are fictional. The similarities

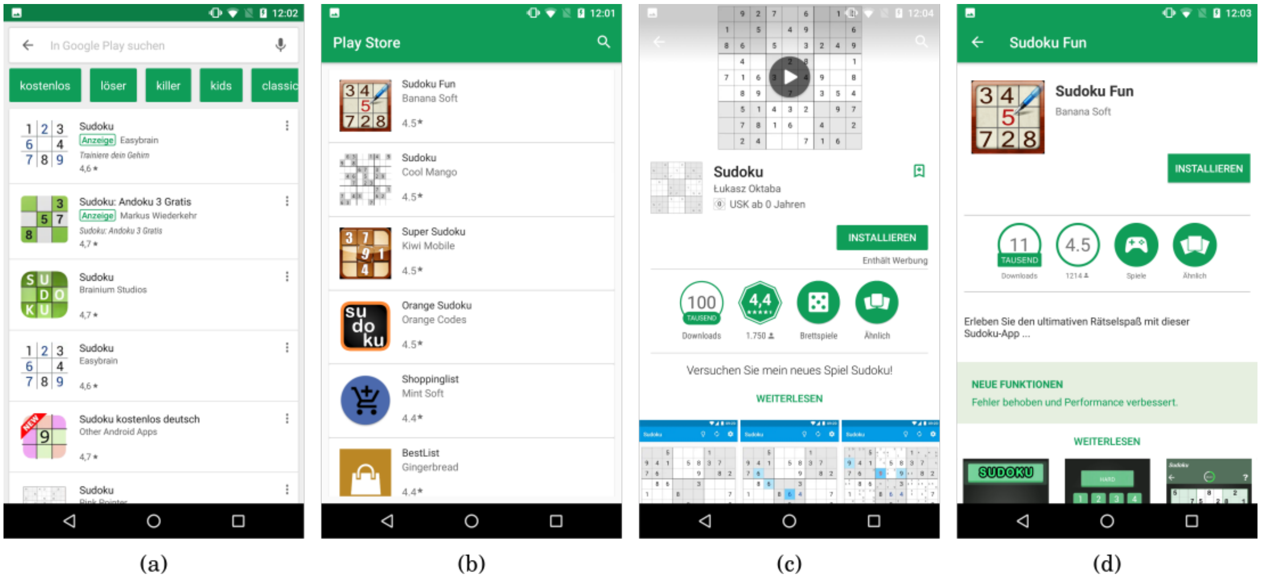

Fig. 2. Screenshots of the original Play Store and or study app. (a) app search in the Play Store, (b) app search in our study app, (c) app details page in the Play Store and (d) app details page in our study app.

and differences in the design of our mock up and the original Play Store are depicted by Figure 2a)-d).

C. Tasks

In each task, the participants were given a description of the functionality the app had to provide, and the mock Play Store provided four apps with a different level of privacy-friendliness according to a certain criterion outlined in the flyer. We investigated only one criterion from the flyer per task and made sure that only this criterion is salient. Therefore, other information that is not criterion-related was kept similar. The criterion-related information was chosen in a way such that there is an objectively best app choice for each task from a privacy perspective. The tasks were designed to evaluate to which extent the participants were willing or able to use the heuristics provided within the flyer in the following way. The objective best choice is always given first.

The objectively best choice is that which, based on the heuristics presented in the flyer, is the most privacy-friendly alternative and at the same time meets all functional requirements. If not all functional requirements are met, the alternative in question is not objectively the best, regardless of how privacy-friendly it is.

1) Task 1 – Permissions: Four Sudoku apps were available here. The apps differed with regards to the permissions they requested upon installation (heuristic ”permissions”):

- requested only non-dangerous[5] permissions,
- requested one dangerous permission not necessary for the functionality
- requested two dangerous permissions that were not necessary for the functionality,
- requested three dangerous permissions that were not necessary for the functionality.

2) Task 2 – Offered versus required functionality: Four shopping apps were available here. The apps differed with regards to the functionally they offered and, correspondingly, the permissions they requested upon installation. All requested permissions were required for the offered functionality, but only one of the alternatives offered exactly the required functionality and therefore requested only necessary permissions (heuristic ”app functionality”):

- the offered functionality equals the required functionality from the instruction,
- the offered functionality is less than required, so fewer permissions are requested compared to the first shopping app but the app does not fulfill all the instructed needs,
- some additional functionality is offered and therefore more permissions are requested compared to first shopping app,
- even more additional functionality is offered and therefore even more permissions are requested compared to the first shopping app.

3) Task 3 – Social metrics: Four audio-recording apps were available here. The apps differed with regards to the number of ratings, the user reviews and the number of downloads (heuristic ”number of downloads”):

- around 450 ratings, 10,000 downloads and only positive reviews,
- around 700 ratings, 14,000 downloads but privacy-related negative reviews present,
- around 450 ratings, 10,000 downloads but privacy-related negative reviews present,
- around 50 ratings, 600 downloads and only one review

[5] We relied on the classification of the permissions into dangerous and non-dangerous in Android as provided at https://developer.android.com/guide/topics/permissions/overview.html\#normal-dangerous accessed on March 10th 2018.

4) Task 4 – Up-to-dateness: Four QR-scanner apps were available here. The apps differed with regards to the date of their last update (heuristic ”on-going development”):

- a few days ago,
- several months ago,
- more than a year ago.
- more than a year ago.

5) Task 5 – Developer: Four mailing apps were available here. The apps differed with regards to the trustworthiness of their developer (heuristic ”developer”):

- a research institution with a user friendly privacy policy that has developed several apps,
- a single researcher with a user friendly privacy policy that has developed only one app,
- a large firm from a country with weak privacy protection laws providing a privacy policy with explicitly stated collection and usage of user data,
- a developer without a website or a privacy policy or other apps.

For Task 1, mock websites for the developers were provided, which the participants could access from the mock Play Store app on the lab smartphone.

D. Participants

Participants were recruited via university mailing lists and student groups on social networks. Each participant was rewarded with 10 Euros for participation. As an alternative, students majoring in psychology at our university had the opportunity to have the trial period credited as test person hours for their studies.

A total of 38 people took part in the study, who were divided equally between the two groups of experiments. A total of twenty male and eighteen female participants participated in the study. The participants were on average 25.03 years old ($SD = 5.97$). Based on self-disclosure during the experiment, the participants had read the flyer sent to them on average 4.91 days ($SD = 2.40$) before the test date. All participants were Android users. Privately seven participants used Android versions older than 6.0. Correspondingly, 31 participants used Android 6.0 or newer.

E. Hypotheses

We aimed to evaluate the following hypotheses in our study:

H_1 Participants who have received the flyer with app selection heuristics show a significantly better decision quality, i.e. they are more likely to choose the objectively best option.

H_2 Participants who have received the flyer with app selection heuristics use significantly more different decision factors for their decisions, i.e. made a more informed decision.

TABLE I. DESCRIPTIVE OVERVIEW OF THE DECISION BEHAVIOUR OF BOTH TEST GROUPS IN ALL FIVE DECISION SITUATIONS. THE OBJECTIVELY BEST DECISIONS ARE MARKED BOLD.

		Control	**Treatment**
Sudoku	Sudoku Fun	3	4
	Sudoku	0	1
	Super Sudoku	5	1
	Orange Sudoku	11	13
Shopping	**Shoppinglist**	12	6
	BestList	2	8
	TopShop	4	1
	CrazyShopping	1	4
Audio-Recording	**RecordPlus**	14	15
	King Record	3	1
	Super Recorder	0	1
	Recording Guru	2	2
QR-Scanner	**Scanning Total**	4	13
	FastQR Scan	10	5
	EasyQR Scan	5	1
	QR Scanning Lite	0	0
Mailing	Unicorn Mail	6	3
	Simple Mail	5	7
	Direct Mail	6	6
	Mailing App	2	3

V. RESULTS

This section describes the results of the study in detail. First, the evaluation with regard to the decisions made and the quality thereof (H_1), then the decision factors used for this purpose (H_2) and finally the time required as well as other control variables are displayed.

A. Decision Quality

In order to analyze the decision behaviour of the participants, the data of the selected app was re-coded so that a 1 stands for the objectively best choice and a 0 stands for all other choices. Table I gives a descriptive overview of the decision behaviour of both experiment groups, with the objectively best choice being marked.

The inference statistical analysis was carried out by means of a variance analysis with repeated measurements. The five decisions made were used as an inner subject-factor and the experimental condition as a between-subject factor. The analysis shows a significant main effect of the between-subject factor ($F = 6.23; p < 0.01$). Individual comparative tests show that the participants from the experimental group decided significantly more frequently ($F = 10.57; p < 0.01$) for the objectively best QR-scanner app. There are no significant differences in the four other decisions ($p > 0.05$). Since the first hypothesis is only correct for one of five scenarios, it must be rejected as a whole.

B. Decision Factors

In order to analyze which information was used by the participants for making their decisions, the self-reports from the interview part of the experiment were first coded accordingly as 1 (correspondingly used) or 0 (not used). Since more could be mentioned in self-reports than actually used to appear better in person, these data were corrected afterwards if necessary on the basis of the screen recordings. For this only 1 to 0 being

TABLE II. Overview of the analysis of the decision time, the days since reading the flyer, the age as well as the information used for the decision of both trial groups; the first two columns provide descriptive data with standard deviation or percentages in parentheses.

		Control	**Treatment**	**F-value**	**p-value**	**part.** η^2
Decision time [seconds]	Sudoku	111.79 (51.21)	145.16 (61.91)	2.883	.098	.074
	Shopping	174.00 (86.22)	182.37 (95.70)	.080	.779	.002
	Audio-Recording	177.58 (63.66)	159.00 (57.92)	.885	.353	.024
	QR-Scanning	144.37 (50.61)	199.32 (145.76)	2.410	.129	.063
	Mailing	165.21 (73.67)	210.26 (102.31)	2.426	.128	.063
Days since flyer read		4.92 (2.52)	4.89 (2.35)	.001	.974	.000
Age [years]		25.47 (6.34)	24.58 (5.72)	.209	.650	.000
Information usage	Developer	2 (11%)	13 (68%)	19.446	.000	.351
	Permissions Installation Dialog	7 (37%)	19 (100%)	30.857	.000	.462
	Permissions Details	4 (21%)	11 (58%)	5.959	.020	.142
	Permissions App-Starting Dialog	1 (5%)	11 (58%)	16.981	.000	.321
	Functionality = Instruction	17 (89%)	16 (84%)	.220	.642	.006
	Downloads	15 (79%)	18 (95%)	2.077	.158	.055
	Reviews	14 (74%)	19 (100%)	6.429	.016	.152
	App Rating	19 (100%)	19 (100%)	N/A	N/A	N/A
	Date of Last Update	2 (11%)	10 (53%)	9.290	.004	.205

changed if the corresponding information was not displayed in the screen recording for at least one second during the decision. For example, if a participant indicated that he or she has taken the permission details of the app into account for his or her decision, but has never looked at the corresponding screen in the Play Store for at least one of the apps, the 1 based on the self-report was coded to 0. This was true in only two cases. No coding from 0 to 1 took place, since the mere display of corresponding information does not necessarily indicate that this information was taken into account in a decision. Forgetting some factors cannot therefore be ruled out. In order to counteract this, the individual factors were also mentioned individually, and their consideration queried.

For the hypothesis test, a multivariate analysis of variance was performed, using the experimental condition as an independent variable and the various information types as dependent variables. Table II shows the results of this analysis in detail as well as the various information types. Participants in the trial group were significantly more likely to use information about the developer, permissions, reviews, and time of the last update. There were no differences in the usage of the download numbers, the fit between the offered functionality and the functional requirements as well as the app rating. The latter was used by all participants from both groups so that no statistical evaluation was possible or meaningful. Since the participants in the experimental group used the individual decision factors exclusively more frequently or equally frequently for their decisions, the second hypothesis can be confirmed.

C. Decision Efficiency and Control Variables

Since the second hypothesis postulates that after reading the flyer more different factors are taken into account for the decision, it seems plausible that the time required for the decision increases, i.e. it becomes less efficient. From a usability perspective, this could have a negative effect on the acceptance of the flyer. In order to analyze the time required by the participants for the respective decisions, these were first determined on the basis of the screen recordings. In each case, the time of the first interaction (e.g., selecting the search field or scrolling in the list) was the starting point. The end point was either the click on the installation button or if the app was subsequently opened by the participant, the confirmation or rejection of the last requested permission, whereupon the respective app displayed a message that the investigator had to be notified.

The inference statistical analysis was carried out by means of a variance analysis with repeated measurements, whereby the time required for the individual decisions was used as an inner-subject factor and the experimental condition as a between-subject factor. This shows a significant main effect of the between-subject factor ($F = 6.37; p < 0.01$). However, individual comparative tests show no significant differences between the two groups for the individual decisions ($p > 0.05$). The detailed results of the individual comparisons can also be found in Table II, which also provides a descriptive data.

Similarly, there were no significant differences between the two groups in age ($F = 0.209; p = 0.65$) or in the number of days since the flyer was read ($F = 0.001; p = 0.974$).

VI. Discussion

The results of our study show, that for the most apps the participants in the treatment group did not choose a privacy-friendlier option. The only exception was the choice of a QR-code app whereby the options differed in their up-to-dateness, and the best option was an app that was updated a few days before the study (as opposed to updates that were several months or years old, or non-existent at all). It therefore is worthy of further investigation, whether the importance of up-to-dateness as a decision factor is generally perceived more important to the end users, and for what reasons.

Still, the two other tasks that did not show any significant differences in decision quality between control and treatment groups, the number of participants who chose a privacy-friendlier option was rather high in both groups. As such, 11 out of 19 participants in the control group (58%) and 13 out of 19 participants in the treatment group (68%) preferred the app with the fewest permissions. Similarly, in the task where the apps differed in their social metrics, the vast majority in both control (74%) and treatment (79%) group chose an app that had the highest number of downloads and reviews, and did not contain any negative reviews regarding privacy. It can therefore be concluded, that the participants were mostly aware of these factors before the study. On the contrary, a relatively low number of participants (26% in the control group, 37% in the treatment group) chose a privacy-friendlier option in the task where the apps differed regarding their developer. One possible reason could be the additional effort required to check the trustworthiness of the developer, i.e. to visit the developer's website and read the information about the developer as well as privacy policies. It therefore remains open to investigate, to which extent the participants' decisions can be improved, if an understandable presentation of the trustworthiness of the developer is provided to the end user.

In the final task, the participants in the control group were more likely to choose an app that requested the fewest permissions while providing all the functionality as outlined in the task description (63% in the control group versus 32% in the treatment group). The participants in the treatment group, on the other hand, preferred the app that requested the fewest permissions out of all options, yet lacked some of the functionality (11% in the control group versus 42% in the treatment group). Hence, many participants in the treatment group chose a privacy-friendlier option, even if they neglected the task description.

Overall, while the flyer did not lead the participants to choosing the objectively best alternatives, it increased their ability to make informed decisions regarding their app choices. Our results show that significantly more participants in the treatment group considered factors that are crucial in determining an app's privacy-friendliness. Such factors are permissions, information about the developer and app reviews. Privacy is not a simple binary state, which can be either true or false. It is a manifestation on the continuum of control over the access and processing of personal information [7] that is evaluated differently by each individual based on personal preferences. Hence, there is no optimum of privacy that is valid globally. On the contrary, it seems to be paramount, that users can process all the information they need with an appropriate amount of resources in order to choose an option that is as optimal as possible for user personally. Even if, from a researcher's point of view, those options not necessarily offer the greatest privacy protection.

A closer look at the participants in the treatment group that decided against the objectively best option reveals other aspects that were taken into consideration by these participants while choosing an app. Those aspects are either not contained in the flyer, such as the design of the app, or are present in the flyer, but do not vary significantly. An example of this would be the number of ratings. This number varied for the aspects in Task 1 between $1,176$ and $1,231$. The privacy-friendlier option, that is the app that required no permissions, had the lowest number of reviews among all aspects, while the apps with a higher number of reviews requested unnecessary and dangerous permissions. It therefore remains open, how the end users decide on the trade-off between the heuristics that is most optimal for their specific needs.

VII. Related Work

A number of works aimed to support users' privacy-related decisions in the smartphone context. One research direction focused on deriving methods for calculating the risk score of an app and visualizing it to the users. This can be either via modifying the interface of an app store or by providing an external service [6], [15], [22], [23]. Depending on the computation of the risk score, a complex analysis might be required (e.g., code analysis and crowd-sourcing in the PrivacyGrade project [15], [23]), and therefore, no decision support will be provided for the apps that have not been analyzed yet. Furthermore, presenting the privacy risk of the app as a single value does not inform the user of different factors that might influence the risk.

Other works focused on modifying the Play Store interface by including additional explanation of the data collected by the app. The proposal by Kelley *et al.* [13] introduces a privacy display with the goal to make the information about data collected by the app more clear to the user. The work by Choe *et al.* [6] uses privacy nudges, informing the user on the amount of time their sensitive information has been shared with apps. A similar approach has been proposed by Balebako *et al.* [2] and provides notices and visualizations to the users that enable them to see when and how often their data has been shared. Harbach *et al.* [11] propose the usage of personalized examples, showing the user which of their stored data will be shared by an app in case they decide to install it. Gerber [10] uses expert recommendations and explaining interactions between different permissions to better inform the user. These works, however, focus on app permissions and do not consider other privacy-relevant factors, such as the trustworthiness of the app developer.

Information materials have been proposed by governmental agencies, such as the German Office of Federation Security [4], the US National Institute of Standards and Technology [20], or the UK National Cyber Security Centre [19], that aim to support either admins or end users in securing their mobile devices. Most of the content of these materials, however, is rather technical, aimed at users with IT-expertise, and to our best knowledge, the extent to which these materials are accessible to lay users has not been independently investigated. Gerber [8] used an interactive training app to increase user knowledge and the awareness of users with respect to privacy related behavior related to their smartphone.

VIII. Conclusion

Since smartphones are used for a variety of tasks, apps could access large amounts of personal and often also sensitive data. Because these data can potentially be misused, it is up to the user to decide whether installing a particular app presents a considerable risk to this user's privacy. While app stores include information about the app that could help estimating privacy risks, the complexity of this information, the confusing user interfaces of app stores and general misconceptions about smartphone privacy prevent users from making informed privacy decisions.

To remedy this situation, we designed information material in the form of a flyer that consists of two parts. The first part deals with common misconceptions of users regarding their privacy in the smartphone context. These misconceptions were identified by literature research and include beliefs that prevented users from adequately protecting their privacy. Examples for misconceptions are the belief that only politicians or celebrities can become targets for attacks on privacy or that apps in official app stores do not pose privacy risks. The second part of the flyer contains various heuristics for choosing privacy-friendlier apps. The heuristics are taken from a previous interview study with IT-security experts about their daily practice in using smartphones and their way of searching and installing apps [14].

We evaluated the flyer in a between-subject lab study with 38 participants. The results show that the participants who read the flyer several days before the study consider privacy-relevant factors more frequently when selecting the apps than the participants in the control group who did not read the flyer. This result suggests that the flyer can improve the ability of participants to make more informed decisions to protect their privacy. Nevertheless, many participants in our study still decided against a more data protection-friendly option when selecting apps, despite considering data protection-relevant factors.

Future work should therefore focus on further exploring participants' preferences and the trade-offs between different decision factors related to privacy when using the smartphone. Furthermore, the heuristics do not consider whether an app is open-source. This information is not present in the app store and the user would have to search for it. However, open-source apps often form a privacy-friendly option, such as the open-source "Privacy Friendly Apps" [16], that advertise with privacy optimization. The impact of the open-source property of an app on the privacy-related decisions should be investigated in future work.

Acknowledgment

This work was partially funded by the European Unions Horizon 2020 Research and Innovation Programme through the GHOST project (https://www.ghost-iot.eu/) under Grant Agreement No. 740923. The research reported in this paper has furthermore been supported by the German Federal Ministry of Education and Research (BMBF) as well as by the Hessen State Ministry for Higher Education, Research and the Arts within CRISP as well as by the German Federal Ministry of Education and Research (BMBF) within MoPPa (16KIS0343). It was also supported by the German Federal Ministry of Education and Research within the Competence Center for Applied Security Technology (KASTEL). This work has been furthermore co-funded by the DFG as part of project "Area D.1" within the RTG 2050 "Privacy and Trust for Mobile Users" and by the Horst Görtz Foundation."

References

[1] M. Alsaleh, N. Alomar, and A. Alarifi, "Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods," *PLOS ONE*, vol. 12, no. 3, p. e0173284, 2017.

[2] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "Little brothers watching you: Raising awareness of data leaks on smartphones," in *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS)*. New York, NY, USA: ACM, 2013, p. 12.

[3] K. Benton, L. J. Camp, and V. Garg, "Studying the effectiveness of android application permissions requests," in *Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. Piscataway, NJ, USA: IEEE, 2013, pp. 291–296.

[4] Bundesamt für Sicherheit in der Informationstechnik, "Überblickspapier Smartphones," https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf?__blob=publicationFile, accessed 24.04.2018.

[5] 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 (SOUPS)*. New York, NY, USA: ACM, 2012, p. 1.

[6] E. K. Choe, J. Jung, B. Lee, and K. Fisher, "Nudging people away from privacy-invasive mobile apps through visual framing," in *IFIP Conference on Human-Computer Interaction*. Cham, Switzerland: Springer, 2013, pp. 74–91.

[7] M. J. Culnan and P. K. Armstrong, "Information Privacy Concerns , Procedural Fairness , and Impersonal Trust : An Empirical Investigation," *Organization Science*, vol. 10, no. 1, pp. 104–115, 1999.

[8] N. Gerber, P. Gerber, H. Drews, E. Kirchner, N. Schlegel, T. Schmidt, and L. Scholz, "Foxit: Enhancing mobile users' privacy behavior by increasing knowledge and awareness [in press]," in *Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. ACM, 2017.

[9] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox : A systematic review of literature investigating privacy attitude and behavior," *Computers & security*, vol. 77, pp. 226–261, 2018.

[10] P. Gerber, M. Volkamer, and K. Renaud, "The simpler, the better? Presenting the COPING Android permission-granting interface for better privacy-related decisions," *Journal of Information Security and Applications*, vol. 34, pp. 8–26, jun 2017. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S2214212616302721

[11] M. Harbach, M. Hettig, S. Weber, and M. Smith, "Using personal examples to improve risk communication for security & privacy decisions," in *Proceedings of the SIGCHI conference on human factors in computing systems*. New York, NY, USA: ACM, 2014, pp. 2647–2656.

[12] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A conundrum of permissions: Installing applications on an android smartphone," in *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*. Cham, Switzerland: Springer, 2012, pp. 68–79.

[13] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, 2013, pp. 3393–3402.

[14] O. Kulyk, P. Gerber, B. Reinheimer, K. Renaud, and M. Volkamer, "Encouraging privacy-aware smartphone app installation: What would the technically-adept do," in *Proceedings of the NDSS Workshop on Usable Security (USEC)*. Reston, VA, USA: Internet Society, Feb. 2016, pp. 1–10.

[15] 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 the 2012 ACM Conference on Ubiquitous Computing*. New York, NY, USA: ACM, 2012, pp. 501–510.

[16] K. Marky, A. Gutmann, P. Rack, and M. Volkamer, "Privacy friendly apps - making developers aware of privacy violations," in *1st International Workshop on Innovations in Mobile Privacy and Security (IMPS)*. CEUR Workshop Proceedings, 2016, pp. 46–48.

[17] A. Mylonas, D. Gritzalis, B. Tsoumas, and T. Apostolopoulos, "A qualitative metrics vector for the awareness of smartphone security users," in *Proceedings of the International Conference on Trust, Privacy and Security in Digital Business (TrustBus)*. Cham, Switzerland: Springer, 2013, pp. 173–184.

[18] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.

[19] National Cyber Security Centre, "Keeping your smartphones (and tablets) safe," https://www.ncsc.gov.uk/guidance/keeping-your-smartphones-and-tablets-safe, 2017, accessed 24.04.2018.

[20] National Institute of Standards and Technology, "NIST Special Publication 800-124 Revision 1. Guidelines for Managing the Security of Mobile Devices in the Enterprise," https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf, 2013, accessed 24.04.2018.

[21] M. E. Poikela and F. Kaiser, "'it is a topic that confuses me'–privacy perceptions in usage of location-based applications," in *Proceedings of the European Workshop on Usable Security (EuroUSEC)*. Reston, VA, USA: Internet Society, 2016, pp. 1–11.

[22] P. Rajivan and L. J. Camp, "Influence of privacy attitude and privacy cue framing on android app choices," in *Twelfth Symposium on Usable Privacy and Security (SOUPS)*. Berkeley, CA, USA: USENIX Association, 2016.

[23] J. L. B. L. N. Sadeh and J. I. Hong, "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *Symposium on Usable Privacy and Security (SOUPS)*. Citeseer, 2014, pp. 199–212.

[24] H. J. Smith, T. Dinev, and H. Xu, "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, vol. 35, no. 4, pp. 989–1015, 2011.

[25] A. Tsohou and E. Kosta, "Enabling valid informed consent for location tracking through privacy awareness of users: A process theory," *Computer Law & Security Review*, vol. 33, no. 4, pp. 434–457, 2017.

[26] M. Volkamer and K. Renaud, "Mental models–general introduction and review of their application to human-centred security," in *Number Theory and Cryptography*. Springer, 2013, pp. 255–280.

[27] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz, "A sociotechnical investigation into smartphone security," in *Proceedings of the International Workshop on Security and Trust Management (STM)*. Cham, Switzerland: Springer, 2015, pp. 265–273.

[28] K. Wolf, K. Marky, and M. Funk, "We should start thinking about privacy implications of sonic input in everyday augmented reality!" in *Mensch und Computer 2018 - Workshopband*. Bonn, Germany: Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, 2018.