Baalous, R. and Poet, R. (2020) Factors Affecting Users' Disclosure Decisions in Android Runtime Permissions Model. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 29 Dec 2020 - 01 Jan 2021, pp. 1113-1118. ISBN 9780738143804.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

http://eprints.gla.ac.uk/234950/

Deposited on: 24 February 2021

Enlighten – Research publications by members of the University of Glasgow
http://eprints.gla.ac.uk

Factors Affecting Users' Disclosure Decisions in Android Runtime Permissions Model

Rawan Baalous
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
r.baalous.1@research.gla.ac.uk

Ronald Poet
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
ron.poet@glasgow.ac.uk

***Abstract*— Today, Android users are faced with several permissions' screens asking to access their personal information when using Android apps. In fact, Android users have to balance several considerations when choosing to grant or deny these data collection activities. Hence, it is important to understand how users' decisions are made and what factors play a role in users' decisions. A number of studies on the permissions' screens of Android devices have reported users discomfort and misunderstanding of the permission system. However, most studies were carried out on the old permission system where all permissions are presented at installation time, and the user has to either accept all the permissions or stop the installation. With the new permission system started with Android version 6.0 and higher, permissions are presented differently at run time. In this work, we aim to study users' disclosure decisions with the new run time system on Android. We have modeled users' disclosure decisions from three perspectives: dangerous permission type, clarity of rationale, and clarity of context. The study has been conducted on Amazon Mechanical Turk. The results show that dangerous permission type as well as clarity of the context have a statistical significant effect on users' disclosure decisions. On the other hand, clarity of dangerous permission's rationale does not contribute significantly to users' decisions. These findings shed light upon important factors that users consider in making privacy decisions in the new Android run time model. Such factors should be taken into account by Android apps developers when requesting access to users' private information.**

Keywords*— *Android runtime, privacy policy, disclosure decisions, Android permissions

I. INTRODUCTION

Despite the fact that privacy is not a new issue for users, the issue is becoming more complex when associated with mobiles. Smartphones are increasingly integrated into people's lives. Large amount of users' personal data are produced and associated with users' activities on mobile devices. This increases the issue of privacy at different levels [1]. In addition, users' personal information has become the currency that is paid by mobile apps' users for several mobile services, such as entertainment and social networking apps. That is, mobile users often accept a number of permissions requests to access their personal data by mobile apps, to be able to use the apps properly. This personal information, such as contacts and call logs are used by mobile apps for different purposes and can be shared with different entities [2].

Accessing to users' private data in Android is done through Android permissions system. In order for an Android app to be able to request authorization to users' personal data, the permissions must be declared in the app's manifest file. Starting from Android version 6.0 (Marshmallow), Google changed the Android permissions model (installation time model) that has been criticized for a long time. Instead of granting all permissions at installation time, permissions can be individually granted or denied at run time. When the app attempts to access user data that might affect user's privacy (dangerous permission), Android will present the permission screen. The user can then choose either to allow access to the data or deny the request. In Android Marshmallow and above, users can still use the app even after denying the requested permission, but maybe with limited functionality. Users can revoke the granted permissions whenever they want, using Android settings [3].

Many previous works have focused on surveying the issues associated with the Android permissions based model. However, most studies were carried out on the old permission system where all permissions are presented at installation time. With the new permission system started with Android version 6.0 and higher, permissions are handled differently and users are given more control over dangerous permissions that affect their privacy. This work aims to benefit from this change by understanding how users' decisions are made and what factors play a role in users' decisions in the new Android permissions model.

Drawing on Nissenbaum's theory of Privacy as Contextual Integrity [4], we investigate the impact of dangerous permission type, rationale of the dangerous permission (extracted from app's privacy policy), and the context of the dangerous permission request on user's disclosure decision. By examining the impact of dangerous permission type (contacts, location … etc.) on users' disclosure decisions, we aim to investigate the resources that users consider highly sensitive. This investigation should help developers to pay increased attention when requesting these permissions and only ask them when they are needed for the app to work. This study also investigates the impact of clarity of dangerous permission's rationale and context on users' disclosure decisions. Studying the rationale and context factors highlight to developers' attention when to request dangerous permissions and how obvious is the rationale as well as permission screen's triggered action. Finally, the study seeks to offer valuable insights for privacy policies writers into the importance of transparency in data handling practices described in apps' privacy policies and its impact on users' privacy decisions.

Toward achieving our goal, we designed a prototype of an Android app and used a vignette survey to shed light upon some factors that could affect users' decision making process. We also asked users about their comfort level associated with each factor as an additional interesting finding. Based on the findings and lessons learned, we provided recommendations for developers in using the new permission system and how to help users to make more informed privacy decisions.

The reminder of this paper is organized as follows: The related work is detailed in Section II. The methodology is discussed in Section III. Sections IV and V detail the results and compare them to previous works. Finally, Section VI presents the conclusion, limitations and future work.

II. Related Work

A considerable body of literature has been focused on studying users' perceptions, behavior and comfort of Android permissions system [5-9]. Several studies also have proposed extensions to Android permissions system and investigated their effect on users' privacy behaviors [10-12]. However, most of the past studies were carried out on the old Android permissions model (before Android version 6.0). As discussed previously, the old permissions model is totally different than the new one. Taking that into account, we are uncertain about the applicability of past studies' results to the new Android permissions model.

A small amount of previous research recently compared the old Android permissions model with the new Android permissions model from users' perceptive. One such study compared the perception and usefulness of three permissions models: Old Android model, run time Android model and iOS permissions model [13]. The results showed that run time permissions are perceived as more useful and positive compared to the old Android model. Peruma et al. [14] examines users' perception and comprehension of the old and new Android permissions model. They found that users perceived the run time model to be slightly more secure than the install time model. The majority of users could recall the permissions requested in the Android run time model more than the install time model.

Some research efforts studied users' satisfaction and concerns about the new Android run time permissions model. One such study [15] explored users' satisfaction with the usability and security of the Android run time model. Most users argued that they have more control over their personal data sharing in the run time model. Another study investigated users' perception and concerns toward the Android run time model by inspecting users' reviews to Android apps in the Google Play Store [16]. Issues related to the lack of permissions rationale messages were prominent in the reviews data. A recurrent issue was about bad request timing, meaning that apps ask for all permissions upfront, instead of following the new run time approach and ask for permissions when users invoke the related functionality.

Considering that users' actual behavior might not reflect their words, a previous work [17] analyzed permissions data in Android devices with the run time model. Then, they compared the collected permissions data which represents users' actual behavior with users' reported privacy preferences. The results revealed that although users are more reluctant to allow specific dangerous permissions such as the microphone or camera, they granted these permissions to particular app categories. This is due to the fact that the gained benefits outweigh the potential risks, or what is called privacy calculus

Closely related to our work [18], the authors investigated users' decision making in the Android run time model. They measured the approval and denial rates of permissions generally, and on each permission type individually. In summary, the approval rates of run time permissions requests (86%) far exceeded the denial rates. As per permission basis, the highest denial rate was associated with microphone access. The top reported reason behind denying run time permissions requests is that the permission looks irrelevant to the app's functionality. On the other hand, the top reported reason behind granting run time permissions requests is the user's desire to use a specific feature that requires this permission.

III. Methodology

In this study, we performed a between-subjects, full factorial vignette survey. Vignette surveys are widely used methods in many disciplines. They are employed to get deep insights into humans' decision making principles. Compared to direct questioning, vignette surveys minimize social desirability bias (SDB), as participants respond to hypothetical situations instead of stating their opinions explicitly. Such surveys are considered less prone to SDB especially in sensitive issues where attitudes are assessed indirectly [19,20]. The vignette study consists of a variety of vignettes. Vignettes are descriptions of objects or situations that are varied experimentally in order to elicit participants' beliefs, attitudes, or intended behaviors [21].

Our vignette study measures the impact of three independent variables: dangerous permission type, clarity of dangerous permission's rationale and clarity of dangerous permission's context on the dependent variable: disclosure decision. The study begins by showing participants a short description of the newly launched Android game app, Citymanage. Citymanage app wants players to build the best city in the world. The player, with the help of his group members, are responsible of constructing the city and managing everything related to it, including public transportation, schools and healthcare. The study then continues by showing how David, a fictional character, plays the app. This is done by presenting participants with a number of scenarios in which David uses the app. Here is an example of a scenario: "As with any new city, laws must be established. Deciding on which laws to activate first is a hard decision as it requires weighing up the advantages and disadvantages. Such decisions need to be discussed between group players. However, it is night time now and David decided to postpone the discussion to tomorrow morning at 10 am. He wanted to add this appointment to his calendar. He pressed the button (add to my calendar) and the following screen appeared". The dangerous permission, clarity of dangerous permission's rationale and clarity of dangerous permission's context differ in these scenarios. Participants are then asked about their disclosure decision in each scenario.

Participants were recruited from Amazon Mechanical Turk. All participants were over 18 years old and have an Android device. Once participants accepted taking the survey, they were redirected to SurveyMonkey online survey tool. Participants took on average 4 minutes and 32 seconds to complete the survey. As the quality of the data obtained relies on the participants [22], we applied a number of qualification tests to ensure high quality data. First, we limited our participants to those with at least 1000 prior tasks accepted with 95% or greater approval rate. Second, we asked our participants to confirm that they have Android device and provide the version of their Android. If the provided version of Android is not correct, the response is rejected. Third, we included an attention question in the middle of the survey, stating: "I am randomly answering the survey" with a "Yes" or "No" answer. Responses answering "Yes" to this question were excluded, in order to reduce the risk of random responses. We also didn't allow the survey to be taken more than once from the same device. In total, 140 participants answered the survey. After running the quality and attention checks, we ended up with 119 responses. Each participant was given $1.00 after successfully answering the survey.

In the following subsections we outline how the rationales of the dangerous permissions were extracted. We also describe the decisions scenarios and survey development. Finally, prototype design is presented.

A. *Dangerous Permissions Rationales' Extraction*

Our dataset contains the top 100 Android apps from Google Play Store. The apps were chosen from all Google Play Store categories to assure saturation of dangerous permissions' rationales and diversity. The privacy policies of these apps were downloaded and dangerous permissions' rationales were manually extracted. We choose to extract the rationales from real privacy policies which reflect actual apps practices related to users' personal information on Android.

In order to extract the rationales of dangerous permissions, we used the list of keywords representing dangerous permissions from [23] and recorded all the dangerous permissions used by the apps and the associated rationale sentences, if any. The process of downloading privacy policies and extracting the rationales took place in September – November 2019.

After that, the dangerous permissions' rationales were classified to clear and vague based on the following definition: "Ambiguity arise when a statement is incomplete and missing relevant information, or when a word or phrase has more than one possible interpretation and the reader is uncertain about which interpretation the author intended" [24]. In order to mitigate threats to construct validity, two other researchers independently participated in reviewing the extracted clear and vague rationales, sentence by sentence, during the privacy policies analysis. We only considered clear and vague rationales where both researchers agreed on.

B. *Decisions Scenarios*

In this study, we developed a set of scenarios varying over three variables: the dangerous permission type, clarity of dangerous permission's rationale and clarity of dangerous permission's context. The full factorial vignette, which contains all the combinations of factors' levels, is 36. However, the number of vignettes is too large to be presented to single participants. In fact, presenting such large number of vignettes to participants might create a risk of boredom or fatigue. In addition, cognitive overload is more evident when participants have to evaluate numerous vignettes. It was found that after around the tenth vignette, participants' attention decreased [20]. Hence, we divided the 36 vignettes into 4 blocks with 9 vignettes each. Participants were randomly assigned to blocks. Vignettes were randomly ordered per participant. This is important to eliminate possible learning effect. Below we describe the three vignette factors in detail.

By dangerous permission type we refer to the nine categories of dangerous permissions in Android: Calendar, camera, contacts, location, microphone, phone, sensors, SMS and storage. For the rationale of dangerous permission, we used two variations: vague and clear, as detailed in the previous subsection. The context of the dangerous permission access could be self-explanatory or vague. By self-explanatory, we mean the dangerous permission access with obvious and immediate triggering action by the app's user. For example, a request for accessing the user's gallery that is prompted when the user pressed "upload photo" button is considered self-explanatory.

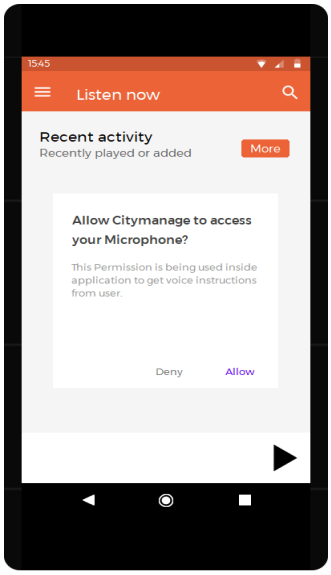


Fig. 1. An example of a permission access screen

C. *Survey Development*

Before running the full survey, the survey was tested by two experts. Then, it was piloted with 14 participants varying in their technical knowledge. Participants were selected from a convenient sample and the survey was updated accordingly. Ethical requirements were in accordance with University of Glasgow ethical guidelines.

Following that, participants were presented with the Android app's description and provided with initial instructions which describe the nature of the tasks. Then, participants were presented with scenarios describing different dangerous

permissions' access with their context and rationales. Participants were asked for their disclosure decision "Deny" or "Allow". We also enquired about participants' comfort level as an additional finding. Comfort level question is a 5-point Likert scale, ranging from "Very comfortable" to "Very uncomfortable". After that, participants were asked about demographic information such as gender, age and educational level. They were also asked about their technical knowledge in using Android.

D. Prototype Design

An example of a permission access screen is shown in Figure 1. The same general layout of Android permissions' screens was used to match the look-and-feel of permissions' screens in real Android apps.

IV. RESULTS

In the regression analysis, we modeled users' disclosure decisions based on three predictor variables: dangerous permission type, clarity of rationale and clarity of context of the resource accessed. For dangerous permission type, microphone was selected as a baseline category based on previous work reporting that microphone permission has the highest denial rates compared to other Android permissions [18]. The baseline category for clarity of rationale and clarity of context is vague. The dependent variable in the model is user's disclosure decision, where "allow" is the baseline category and "deny" is the target category.

Table I shows the contribution of each predictor variable to the model as well as its statistical significance. The odds ratio (OR) column presents each variable's observed effect. The values in the OR column can be interpreted as the change in odds of disclosure decision for every one unit increase in the predictor variable. For example, the odds ratio for sensors dangerous permission indicates that for every one unit increase on this predictor, the odds of denying dangerous permission change by a factor of .403 compared to the baseline, microphone dangerous permission, assuming all other predictor variables are kept constant. Since the value of OR is less than one, this means that the odd is decreasing. In other words, users are less likely to deny sensors dangerous permission request compared to microphone dangerous permission request. Similarly, the odds ratio when the context of dangerous permission is clear (self-explanatory) indicates that for every one unit increase on this predictor, the odds of denying the permission change by a factor of .518 compared to when the context is vague, meaning that users are less likely to deny dangerous permission requests when the context is clear compared to when the context is vague. For each OR value, we chose 95% confidence interval (CI) to determine the statistical significance. The CI when the context is clear, for example, indicates that the true odds ratio is between .404 and .663 with 95% confidence. As can be seen from the table, dangerous permission type and clarity of context (p=.000) is less than our significance threshold (p=.05), hence these two predictors added significantly to the disclosure decision model. On the other hand, the clarity of rationale (p=.185) did not add significantly to the model.

TABLE I. SUMMARY OF REGRESSION ANALYSIS OVER DISCLOSURE DECISIONS

Variable	Sig.	OR	95% CI for OR	
			Lower	Upper
Dangerous Permission Type	.000			
Calendar	.113	.656	.390	1.105
Camera	1.000	1.000	.596	1.677
Contacts	.426	1.234	.735	2.072
Location	.314	.766	.456	1.287
Phone	.113	1.526	.904	2.575
Sensors	.001	.403	.235	.692
SMS	.826	.944	.563	1.583
Storage	1.000	1.000	.597	1.674
Clarity of Rationale(Clear)	.185	.845	.659	1.084
Clarity of Context(Clear)	.000	.518	.404	.663

With respect to dangerous permission type, as can be seen in Figure 2, we observed that 61.34% of respondents who were asked to access their phone (phone dangerous permission) denied the request. Following phone dangerous permission, contacts dangerous permission has the second highest denial rates (56.30%). On the other hand, sensors dangerous permission has the highest acceptance rates among respondents (69.75%), followed by calendar dangerous permission (60.50%).

Regarding clarity of the dangerous permission's rationale, surprisingly, differences between clear and vague explanations are not statistically significant, as presented in Table I. Additionally, Figure 3 visually presents users' disclosure decisions. As can be seen, for example, out of all respondents who granted dangerous permissions requested, 53.1% were presented with clear dangerous permissions' rationales and 46.9% were presented with vague rationales. Possible hypothesis behind users' decisions are illustrated in detail in the discussion section.

For clarity of context, as expected, if the context of accessing dangerous permission is clear, users would significantly grant more dangerous permissions requests (58.20%) than they would do if the context of the resource access was unclear (41.80%). Figure 4 reflects the differences in users' disclosure decisions. Referring again to Table I, we can see that the clarity of context contributes significantly to users' disclosure decisions.

Overall, Users' comfort levels were in line with their disclosure decisions. Dangerous permissions with highest denial rates have also the highest uncomfortable level, and vice versa. For example, in the contacts dangerous permission, 60.50% selected very uncomfortable or somewhat uncomfortable, compared to 27.73% in the sensors dangerous permission. When comparing comfort level in relation to clarity of dangerous permission's rationale, out of all respondents who selected very uncomfortable, 53.2% were presented with vague rationales and 46.8% were presented with clear rationales. Further, dangerous permissions requests scenarios where the context of the resource access is vague are associated with higher discomfort levels compared to the clear context condition. These results provide additional insights into

the possible relation between users' disclosure decisions and their comfort level, as Android users may be more willing to deny uncomfortable dangerous permissions requests.

Fig. 2. Acceptance and denial percentages per dangerous permission.

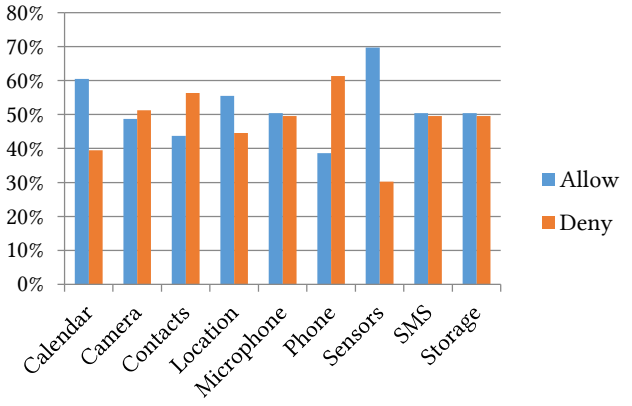


Fig. 3. Acceptance and denial percentages organized by clarity of rationale.

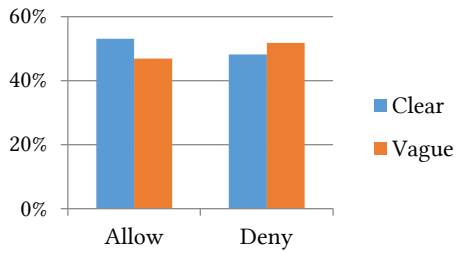
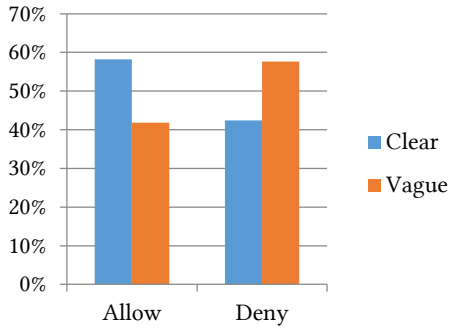


Fig. 4. Acceptance and denial percentages organized by clarity of context.



Regarding participants' demographics, of 119 respondents, over two-thirds (71%) were male and (29%) female. Just over half of the participants aged between 25 and 34 years old. Their level of education varied from having high school degree or equivalent (14%), some college but no degree (15%), associate degree (9%), bachelor degree (52%) and graduate degree (10%). Participants also have varied levels of employment status, with the majority (83%) being employed.

Turning to participants' technical background, a minority of participants (12%) stated that they use their Android device 8 or more hours, while most of them (88%) use it 7 or less hours. When asked to report their expertise using Android device, (50%) regarded their expertise as excellent, (35%) very good, (13%) good and (2%) fair. Finally, in response to the question about their Android device version, the responses show that the majority (90%) are using the new Android run time permission system (starting from Android Marshmallow to Android version 10).

V. Discussion

It has been reported that ambiguity in privacy policy sentences can mislead users and increase privacy risks accordingly [25]. We found that users grant more permissions requests (53.10%) when the provided rationale message is clear, compared to (46.90%) when the provided rationale is vague. However, the regression analysis found this difference to be not statistically significant. A potential explanation is that users may pay more attention to the context in which the permission request occurred, which reveals the more likely rationale, instead of reading the rationale message. Hence, they might ignore reading the rationale message if the context of the resource access request was clear. Consequently, they could rely on the clarity of the context in their disclosure decision more than the rationale message. To clarify, a dangerous permission request to access the device storage after user clicking on "upload photo" button might clearly communicate that the app wants to access the storage to upload the photo. Therefore, a user might accept the permission request according to the clarity of the context without reading the rationale message which could reveal other usage purposes. Consequently, a user relying on the clarity of the context solely may realize that his perception was incomplete when reading what the permission will also be used for in the rationale message. Taking that into account, developers should follow Google guidelines in being transparent and clear about the resources accessed and why.

Related to our work, a previous study [26] examined the impact of presenting purposes messages on Apple iOS users' behavior. The authors assessed developers provided explanations on users' decision making. Participants were presented with screenshots of real apps with their rationale messages and screenshots of other apps with their rationale messages removed. The findings revealed that the approval rate when the purposes messages are shown is 73.6%, and 65.8% when purposes messages are not shown. The authors reported that this difference is statistically significant. This demonstrated that users are more willing to accept permissions requests when rationale messages are presented. Different to our study, the authors did not examine the impact of clarity of purposes on users' disclosure decisions.

Dangerous permission type had a significant effect on users' disclosure decisions. Contacts for example had the second highest denial rate. One possible explanation is that users consider this resource to be highly sensitive. This is similar to the findings of [27] in which participants reported the sensitivity of the resource to be accessed as the reason of denying some permissions requests regardless of whether the app needs the permission to function or not.

Studying the impact of clarity of the context on users' disclosure decisions revealed that this factor is statistically

significant. The findings support the previous literature [18,27] which noticed that relevance to app's functionality is a main reason for granting or denying permissions requests. In fact, clarity of the context may uncover the potential related functionality and show in real time why the app needs to access the dangerous permission. This finding should motivate developers to avoid asking all dangerous permissions upfront and ask them when needed to give users more contextual information that help them in making informed decisions.

VI. Conclusion

In this work, we examined the effect of three factors: dangerous permission type, clarity of dangerous permission's rationale and clarity of dangerous permission's context on users' disclosure decisions in the new Android run time model. The statistical results emphasize that both dangerous permission type and clarity of context have a statistically significant effect on users' disclosure decisions. Although vague dangerous permissions rationales were associated with more denial rates compared to clear rationales, the regression analysis found that the clarity of rationale does not contribute significantly to users' disclosure decisions.

The experiment in this paper is limited as participants did not install the app on their devices and make disclosure decisions in the real world. Future work could include studying other factors such as users' privacy concerns.

References

[1] Zhou, Y., Piekarska, M., Raake, A., Xu, T., Wu, X. and Dong, B., (2017). Control yourself: on user control of privacy settings using personalization and privacy panel on smartphones. Procedia Computer Science, 109, pp.100-107.

[2] Wottrich, V.M., van Reijmersdal, E.A. and Smit, E.G., (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. Decision Support Systems, 106, pp.44-52.

[3] Gasparis, I., Aqil, A., Qian, Z., Song, C., Krishnamurthy, S.V., Gupta, R. and Colbert, E., (2018), May. Droid M+: Developer Support for Imbibing Android's New Permission Model. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security (pp. 765-776). ACM.

[4] Nissenbaum, H., (2004). Privacy as contextual integrity. Wash. L. Rev., 79, p.119.

[5] Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E. and Wagner, D., (2012), July. Android permissions: User attention, comprehension, and behavior. In Proceedings of the eighth symposium on usable privacy and security (p. 3). ACM.

[6] Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N. and Wetherall, D., (2012), February. A conundrum of permissions: installing applications on an android smartphone. In International conference on financial cryptography and data security (pp. 68-79). Springer, Berlin, Heidelberg.

[7] Benton, K., Camp, L.J. and Garg, V., (2013), March. Studying the effectiveness of android application permissions requests. In 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops) (pp. 291-296). IEEE.

[8] Reinfelder, L., Benenson, Z. and Gassmann, F., (2014), September. Differences between Android and iPhone users in their security and privacy awareness. In International Conference on Trust, Privacy and Security in Digital Business (pp. 156-167). Springer, Cham.

[9] Ramachandran, S., Dimitri, A., Galinium, M., Tahir, M., Ananth, I.V., Schunck, C.H. and Talamo, M., (2017), October. Understanding and granting android permissions: A user survey. In 2017 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[10] Kraus, L., Wechsung, I. and Möller, S., (2014), July. Using statistical information to communicate android permission risks to users. In 2014 Workshop on Socio-Technical Aspects in Security and Trust (pp. 48-55). IEEE.

[11] Wang, N., Zhang, B., Liu, B. and Jin, H., (2015), August. Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions. In Proceedings of the 17th international conference on human-computer interaction with mobile devices and services (pp. 373-382). ACM.

[12] Rajivan, P. and Camp, J., (2016). Influence of privacy attitude and privacy cue framing on android app choices. In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016).

[13] Reinfelder, L., Schankin, A., Russ, S. and Benenson, Z., (2018), September. An Inquiry into Perception and Usage of Smartphone Permission Models. In International Conference on Trust and Privacy in Digital Business (pp. 9-22). Springer, Cham.

[14] Peruma, A., Palmerino, J. and Krutz, D.E., (2018), May. Investigating user perception and comprehension of android permission models. In Proceedings of the 5th International Conference on Mobile Software Engineering and Systems (pp. 56-66). ACM.

[15] Andriotis, P., Sasse, M.A. and Stringhini, G., (2016), December. Permissions snapshots: Assessing users' adaptation to the Android runtime permission model. In 2016 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6). IEEE.

[16] Scoccia, G.L., Ruberto, S., Malavolta, I., Autili, M. and Inverardi, P., (2018), May. An investigation into Android run-time permissions from the end users' perspective. In Proceedings of the 5th International Conference on Mobile Software Engineering and Systems (pp. 45-55). ACM.

[17] Andriotis, P., Li, S., Spyridopoulos, T. and Stringhini, G., (2017), July. A comparative study of android users' privacy preferences under the runtime permission model. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 604-622). Springer, Cham.

[18] Bonné, B., Peddinti, S.T., Bilogrevic, I. and Taft, N., (2017). Exploring decision making with Android's runtime permission dialogs using in-context surveys. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (pp. 195-210).

[19] Auspurg, K. and Hinz, T., (2014). Factorial survey experiments (Vol. 175). Sage Publications.

[20] Engel, U., Jann, B., Lynn, P., Scherpenzeel, A. and Sturgis, P. eds., (2014). Improving survey methods: Lessons from recent research. Routledge.

[21] Steiner, P.M., Atzmüller, C. and Su, D., (2016). Designing valid and reliable vignette experiments for survey research: A case study on the fair gender income gap. Journal of Methods and Measurement in the Social Sciences, 7(2), pp.52-94.

[22] Cavanagh, G.F. and Fritzsche, D.J., (1985). Using vignettes in business ethics research.

[23] Baalous, R. and Poet, R., (2018), September. How Dangerous Permissions are Described in Android Apps' Privacy Policies?. In Proceedings of the 11th International Conference on Security of Information and Networks (pp. 1-2).

[24] Reidenberg, J.R., Bhatia, J., Breaux, T.D. and Norton, T.B., (2016). Ambiguity in privacy policies and the impact of regulation. The Journal of Legal Studies, 45(S2), pp.S163-S190.

[25] Bhatia, J., Breaux, T.D., Reidenberg, J.R. and Norton, T.B., (2016), September. A theory of vagueness and privacy risk perception. In 2016 IEEE 24th International Requirements Engineering Conference (RE) (pp. 26-35). IEEE.

[26] Tan, J., Nguyen, K., Theodorides, M., Negrón-Arroyo, H., Thompson, C., Egelman, S. and Wagner, D., (2014), April. The effect of developer-specified explanations for permission requests on smartphone user behavior. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 91-100). ACM.

[27] Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D. and Beznosov, K., (2015). Android permissions remystified: A field study on contextual integrity. In 24th {USENIX} Security Symposium ({USENIX} Security 15) (pp. 499-514).