# Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices*

Prashanth Rajivan
Department of Social & Decision Sciences,
Carnegie Mellon University
Pittsburgh, PA, USA
prajivan@andrew.cmu.edu

Jean Camp
School of Informatics & Computing,
Indiana University
Bloomington, IN, USA
ljcamp@indiana.edu

## ABSTRACT

Transmission of personally identifiable information from smartphone apps has become ubiquitous as smartphones themselves. Privacy controls provided in the form of permissions warnings falls insufficient especially for communicating risk during app installation. Presenting easy to understand privacy risk icons/cues would help people make low risk app choices. However, the human factor requirements for designing such privacy risk icons are largely unknown. Towards this, we conducted a user experiment with 480 participants who made a series of app choices with/without privacy priming and with/without privacy risk communicating icons. Overall, presenting risk communicating icons along with app benefit icons had a significant effect on user app choices in terms of risk-benefit trade-off. We found that one type of privacy icon framing led to mediocre app choices under particular conditions. We found that priming for privacy led to increased concern while choosing apps but did not have an augmenting effect on final app choices when combined with certain type of privacy framing. We conclude by proposing human factor based recommendations for designing privacy risk communicating icons.

## 1. INTRODUCTION

Smartphones have now become a source of continuous personal data for businesses, advertising services and even malicious third parties. Much of this data stream originates from apps and data-driven, personalized services running on smartphones and includes personally identifiable information such as location information, search queries, personal messages, personal media (e.g photos and videos), health information (health tracking information) and financial information. While governmental and corporate location tracking and data compilations (such as with metadata) have led to widespread distress, many users are unaware of the amount of personal data sent to unknown third parties from their own smartphones. High profile events, such as the indictment of the CEO of Stealthgenie [26], sometimes bring these issues to the fore. However, such apps' based privacy risks still remains largely vague to users making app installation decisions on a day-to-day basis.

*Prashanth Rajivan performed this work while at Indiana University, Bloomington.


*Symposium on Usable Privacy and Security (SOUPS)* 2016, June 22–24, 2016, Denver, Colorado.

Surveys have long indicated that individuals value their online privacy [29] but research about users' beliefs with respect to privacy implications of their own behaviors shows a disconnect between belief and reality [21, 20]. Thus, not surprisingly, research focused only on behavior shows that people do not act in a privacy-preserving manner which is inconsistent with their expressed preferences. One of the reasons for such a differential user behavior is information asymmetry and users' uncertainty about the data collected by software services in the background [2]. Also, privacy preferences are not isolated but rather a function of the benefits of sharing information.

Desirable personalization through data compilations is common in smartphone applications. However, usage of personal information in direct opposition to users' privacy preferences is also common. Excessive access to personal information by apps has been found in both iOS [15, 4] and Android [18, 8, 17, 36, 5]. Disclosure of information for obtaining personalized services can therefore be characterized as privacy bargain ideally made through risk/benefit trade-off [1, 25, 33]. In some cases, such a bargain is necessary, benign, and even desirable but in other cases it could lead to invasion, discrimination, and even exclusion [2]. Making an informed, risk aware app installation decision based on risk/benefit trade-off analysis poses as a difficult task for general users because risk and benefits of Android apps are often intangible and asymmetric [22].

Different OS providers use different approaches to inform customers about privacy risks. Google in their Android OS presented a complete list of permission warnings after app selection and before installation. The list was entirely based on the information present in a manifest provided by the developer. However with Android 6.0, Google has adopted Apple iOS like permissions model wherein permission warning prompts are presented at the first access to a certain resource by an app. Such run time warnings are known for habituation effects in users causing them to ignore and click through warnings [35, 16]. Neither permissions-based model has proven to be effective in communicating risk to the users [4].

For usable and secure mobile systems, it is imperative that risk is communicated only when user intervention is absolutely necessary (when risk is unavoidable or when user preference/decision is required to proceed) [14]. When necessary, risk must be communicated early on in the decision making process along with other relevant decision variables [24, 31]. Following these simple, user-centric principles would empower all users to make quick and low risk app choices with little to none uncertainty. Excessive risk warnings during and after installation will only lead to habituation and consequently disregard from users.

In this paper, we present our investigation on the effect of prim-

ing for online privacy and privacy risk communicating icons on user risk behavior during app installation in Android. We investigated the interacting effects of privacy risk communication and privacy priming on user app choices measured in terms of risk-benefit trade-off. We compare effectiveness of two types of privacy icon designs. We conclude by proposing human factors based recommendations for designing privacy icons for smartphone apps.

## 2. RELATED WORK

Android users have to pay attention to permission warnings, read and comprehend them to consequently make risk-aware app installation decision but past research has shown that people usually ignore or pay little attention to the permissions warnings in Android [19]. It was found that only 17% of participants self-reported to have paid attention to the permissions and 42% of participants were even unaware of the existence of permissions. One of the primary reasons for such a user behavior could stem from users' habituation to warning dialogs wherein users have habituated to ignore digital warnings in general [32, 35, 16, 10]. Similarly, due to habituation, past research has also found that users click through most of the smartphone permissions warnings and therefore gain no awareness about the resources being used by the apps [12, 9]. Such a lack of awareness is not constrained to Android based phones but also to other smartphone operating system platforms such as Apple iOS [28]. In addition to users' inattention towards permissions warnings, past research have also found that Android users do not fully comprehend the permissions presented to them during the application installation process [19]. They found that only a few participants carefully read the permissions requested and made decisions about whether to install an app or not based on the permissions requested by the application. One reason for such a seemingly risk seeking behavior is that majority of smartphone users are security naive and therefore are not qualified to make an informed decision considering all the security risks. Hence they require simpler, easy to comprehend, visual cues to make risk averse app choices on a day to day basis.

Past work on risk communication in Android has focused on divergent approaches to improve the permissions interface which includes using simplified text [7], explanations with additional text [24], explanation of warnings with examples [23] and also using visual cues that represents the threat level of the permissions requested [7, 13, 11]. Past research particularly on visual cues has compared framing [34] of visual cues: negative framing versus positive framing. In one research [13], subjects were asked to compare positive framing of risk communication against negative framing and found that presenting visual cues with positive framing differed significantly from negative framing on how users made risk based app decisions. In this experiment, the effect of framing was measured by presenting subjects with the same app repeatedly and by asking to make a comparison between the two scales (negative and positive). In another research [11] subjects were asked to make choices either based on positive framing or negative framing of risk and found that subjects made better choices with positive framing in comparison to negative framing. However, the experiment did not have a control condition to compare the effectiveness of presence of risk cues against no visual risk cues. Hence, it is inconclusive from little past research whether framing of privacy cues has a significant effect on app choices. We also hypothesize that there are other variables at play here that mediates the effect of privacy risk framing on app choices such as individuals' privacy attitudes. Past work on permission warning design in Android[19] has theorized the importance of privacy attitudes and motivation but there has been little to none empirical work on its effect on Android app choices. To fill this gap, we conducted an Internet-based user experiment to measure the influence of privacy priming and privacy risk framing on Android app choices.

## 3. METHOD

An interactive Android play store simulation was developed for the experiment. It was a simulation of play store as in Android v5.0 (a.k.a lollipop) in which the list of app permissions is displayed just before app installation. At the time of experiment, Google's new permission model in Android v6.0 (a.k.a Marshmallow) was not unveiled and therefore was not explored. This system (see Figure 1) was a simulation of play store interfaces and navigation capabilities used in exploring and installing apps on Android based phones. The simulation system was designed using actual images

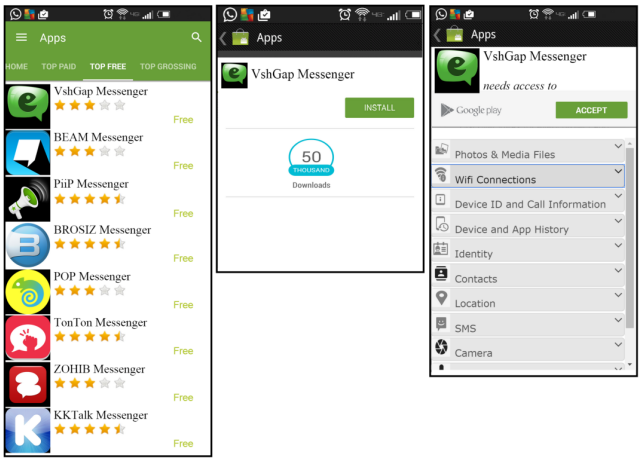


Figure 1: Screenshots of the three simulated Android play store interfaces

of Google play store and images used by real apps on play store. The simulation included three main screens used during app installation decision process: page with the list of apps, individual app description page and app permissions page. Similar to real world play store, the first page on simulation showed a list of apps belonging to a certain category. On selecting an app, the second page with corresponding app details and download count was displayed. Finally, when the user chose to install an app, the corresponding permissions page was displayed. At this point, the participant had two choices, to either install the app or go back to the list of apps. On choosing to install, the participant was taken back to the screen containing list of apps but with a status message "installed" appearing next to app that was chosen as it appears in the actual play store interface. Furthermore, the permissions for a category of apps were based on actual permissions requested by the apps in that category. The system was fully interactive such that the participants had the ability to go back and forth between pages as they would do on actual Android phones. They were also allowed to change their choices and uninstall the previously installed apps. The participant could uninstall and install other apps in a particular category until he/she moves on to make choices in the next category of apps.

For experimental control and to reduce confounds arising from differences in screen size and layout, participants were instructed to perform all the experimental tasks using an Internet browser on a desktop/laptop machine with the simulation interface centered and scaled to the size of a standard large smartphone screen dimensions. Furthermore, only native Android users or users with Android OS

experience was encouraged to participate in the experiment to reduce confounds that might stem from lack of familiarity with Android OS. This was achieved by using a questionnaire based screening process at the start of the experiment.

## 3.1 Apps

Apps used in the simulation were actual apps from Google play store. Apps that were ranked 75 and above on the Google play store at the time of experiment was chosen for simulation to reduce biases in choices due to app popularity and recognition. Apps belonging to eight categories of apps were used in the simulation and they were: “Password Manager", “Ebook Reader", “File Manager", “Messenger", “Puzzle Games", “Fitness", “Dating" and “Photo Editor". For each category, eight number of apps were presented to the participant.

Figure 2: Screenshots of the three risk cues used in the experiment. Risk cues were presented alongside app ratings in the app list page.

## 3.2 Privacy Risk Cues

We compared three different visual cues (Figure 2) for communicating privacy risk: None, Emoticons, Eyes and Padlocks. No visual cue to communicate privacy/risk was the control condition. Emoticon based cue was included in the experiment because emoticons are the widely used modes of social cues for online communication by smartphone and Internet users. Cue with eyes was included because it is also a type of social cue that is innately used to identify human emotions [3]. Finally, padlock was included in the experiment because it has been shown that mental models of non-experts in security overwhelmingly associate computer security with physical security [6]. The two social cues (Emoticons and Eyes) were presented on the risk scale whereas Padlock (security mental model based cue) was presented on the privacy scale. The risk scale was negative framing wherein higher values on the scale represented higher risk (less privacy) and lower values represented lower risk (more privacy). On the other hand, privacy scale was positive framing wherein higher values on scale represented more privacy and lower values on the scale represented less privacy.

## 3.3 Privacy Priming

Privacy Attitude (concern for online privacy) was manipulated by priming participants about online privacy before they performed app choices in the simulation environment. Privacy priming in this experimental context was done using a concise version of the IUIPC (Internet Users’ Information Privacy Concerns) questionnaire [27]. Text or video based descriptions to prime for privacy concerns was not used because memory recall (about individual’s concern for privacy) would be better through test like instruments [30] such as the IUIPC scale. The goal was to prime the users for privacy to augment their concern for privacy online.

## 3.4 Experiment Design

The experiment was a 4X2 between subjects experiment design. The framing of visual cues to communicate privacy/risk score was one of the independent variable and it had four levels. The four levels of privacy/risk cue includes no cue, frown face, human eyes and padlock. Privacy priming was the other independent variable and it had two levels: Privacy primed and not-primed for privacy.

## 3.5 Experiment Procedure

480 participants from Amazon mechanical turk participated in the study of which 233 were females and 247 were males with an average 31 years of age. Participants at the start of experiment (after accepting “HIT" on MTurk) responded to questions about their age and familiarity to different smartphone operating systems (such as iOS, Android and WINDOWS). Participants who self-reported their age to be above 18 and who self-reported to be familiar with the Android OS were only allowed to participate in the experiment. Participants were presented with information about the study and was informed that taking part in this study was voluntary. Participants, on providing consent to participate, were randomly assigned to one of the 8 experimental conditions such that there were 60 participants in each condition at the end of the study. On completion, all participants were paid $2.50 for their participation in the experiment. The study procedures were approved by Indiana university’s Institutional Review Board (IRB) for human subjects’ research.

Based on the experimental condition assigned, fifty percent of the participants were presented with the privacy priming questionnaire (IUIPC privacy questionnaire [27]) at the start of the experiment. Remaining participants did not receive the IUIPC privacy questionnaire. The next step in the experiment involved using the Android play store simulation environment to make several application choices. Prior to using the simulation environment, participants were provided specific but simple set of instructions on using the simulation environment. Since only native Android users were encouraged to participate, the learning curve to get accustomed with the system was hypothesized to be short. In the simulation, the participants were presented with eight categories of apps with eight apps in each category displayed in a randomized order. Each category of apps were presented to the participant one after another. Two levels for each of the three experiment variables: app rating, privacy/risk score and download count, were used as attributes for apps in the simulation environment, making the possible number of variable combinations to be 8 ($2^3$). The 8 combinations of the variable set app rating, privacy/risk score, download count) were randomly assigned to the 8 apps in each category such that each app in a particular category had exactly one of the 8 possible variable set combinations. App rating and risk score ranged between 1 and 5 with two levels: 2 represents low-medium app rating/low-medium risk score and 4 represents high-medium user rating/high-medium risk score. Similarly two levels of download count was used: fifty thousand and hundred thousand downloads. Very low or very high app rating or risk score values such as 1 and 5 were not used. Similarly very low or high download values such as in hundreds or in millions were avoided. This was done to ensure the attributes associated with apps were realistic and also to recreate the complexity of making risk benefit trade-off decisions with real world apps. Participants were instructed to choose 4 of the 8 available apps to install in each category. After the selection of 4 apps in a particular category, the participant had the option to move to the next category containing next set of apps. There was no rigorous time constraints placed on participants to make the four app choices in each category. Participants were given upto an hour to complete all the experimental tasks.

Participants were specifically instructed to choose 4 apps in each category because only 4 of the 8 combination of variables has atleast two variables with desirable values (e.g., high app rating, low risk or high download count) and the remaining 4 apps would have one

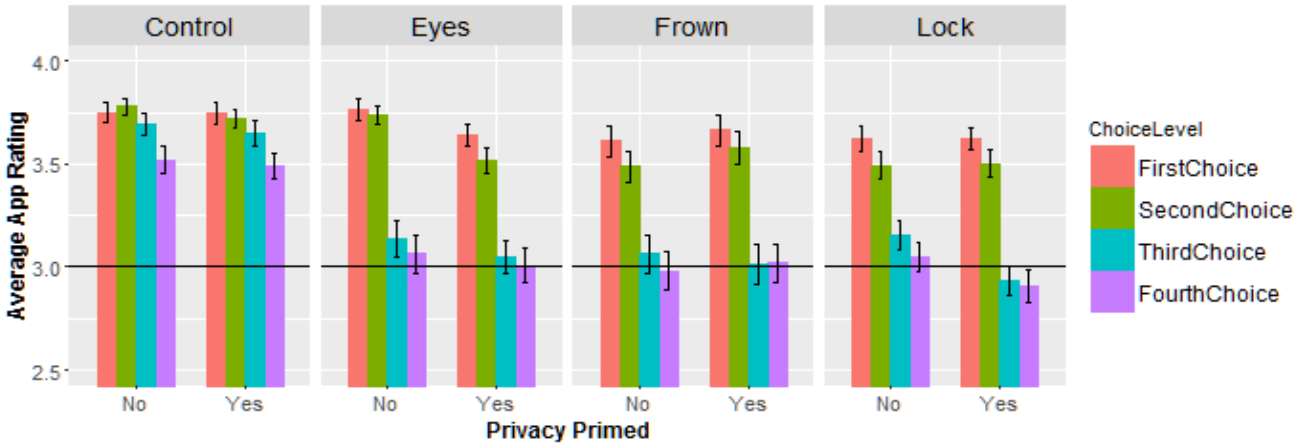


Figure 3: Mean values of app rating of choices across the eight experimental conditions. Horizontal black line is for mid-point reference.

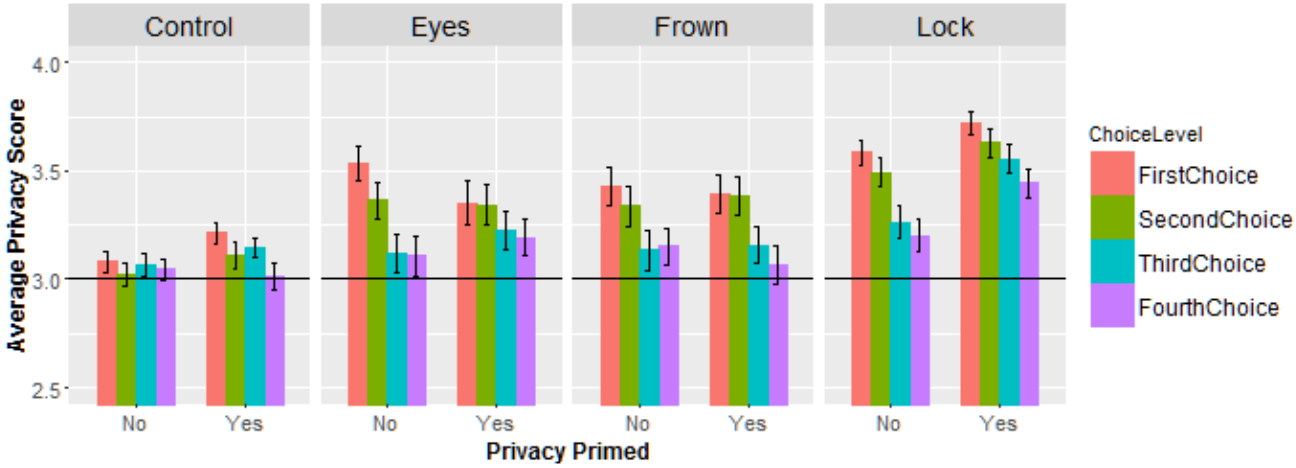


Figure 4: Mean values of privacy score of choices across eight experimental conditions. Horizontal black line is for mid-point reference.

or none of the variables with a desirable value. Hence, having participants select 4 apps as opposed to choosing one or two apps per category would help in measuring the extent of effect of cue and/or priming on app choices. With each app choice, the availability of good app choices reduces leading to choice complexity especially while choosing the fourth app. If the effect of cue and/or priming is strong, it can be hypothesized that the participants would choose all four apps with desirable risk and benefits values.

## 4. RESULTS

We received responses from almost equal percentage of males and females (48.65%) between the ages of 18 to 75. The average age of participants was 31 years. Data from 42 participants were excluded from analysis because they either chose only the top 4 appearing apps for more than 4 categories and/or completed the entire study in a very short duration (under 5 minutes). These metrics were used as indicators for participant's lack of cognitive effort put towards making app choices. Analysis was conducted on data from the remaining 438 participants.

App choices were recorded as a set of three app variables (app rating, privacy/risk score and download count) at each of the 4 choice levels (First, Second, Third and Fourth choices). Analysis was conducted at each of the four choice levels to measure the strength of the effect of risk communicating cues and privacy priming on app choices. The three dependent app variables (app rating, privacy/risk score and download count) were recorded on different scales in the simulation. Therefore, values for all three variables measured from all experiment conditions were normalized to be in the same range of 2 to 4 with 2 representing app choices with low-medium app rating/low-medium privacy score/low-medium download count and 4 representing app choices with high-medium app rating/high-medium privacy score/high-medium download count. Then, for each participant and at each choice level, the privacy score, app rating and download-count values of chosen apps were averaged across the 8 categories of apps. Since values of three app variables were either 2 or 4, on averaging, the mean values close to 2 and 2.5 (floor) indicate that the majority of app choices were of low app rating or less privacy offered (or high risk) or less downloaded. Mean values close to 3.5 and 4 indicates that the majority of app choices were of high app rating or high privacy offered or more downloaded. Finally mean values around 3 indicates inconclusive/indeterminate choices (a combination of high and low choices) where the choices don't excel either in terms of app rating or privacy or download count.

Figure 3 is a graph of mean values of app rating for all four app

choices in all eight experimental conditions. As it can be seen, app rating of all four app choices in the control condition (when primed or not primed for privacy) was between 3.5 and 4 which indicates a strong influence of app rating in all four choices in the control conditions (when there are no cues to communicate risk). In conditions containing risk cues (both risk and privacy framed cues), app rating of the first two app choices was between 3.5 and 4 indicating the influence of app rating whereas the mean app rating of third and fourth app choices in these conditions were close to 3 indicating inconclusive effect of app rating on third and fourth app choices. Mean values of download count for all four app choices in all eight experimental conditions was analyzed. Mean download count of chosen apps was found to be close to 3.0 across all eight conditions indicating inconclusive effect of download count on all app choices. Figure 4 is a graph of mean values of privacy score for all four app choices in all eight experimental conditions. As it can be seen, mean privacy score for all four choices in the control condition (both primed and not primed for privacy) is close to 3. Although, the privacy score of choices in primed control condition is marginally higher than privacy score of choices in non-primed control condition. In comparison, mean privacy score of app choices in the three conditions with risk communicating cues has a lot more variability between conditions. Specifically, in the condition which used padlock for risk communication and also primed participants for privacy, the privacy score of all four app choices was close to 3.5 indicating a strong influence of privacy score on app choices. In comparison, in other conditions with risk cues, we don't observe such a strong influence of privacy score on all four app choices.

The three variables (app rating, privacy score and download count) that describe the app choices were found to violate normality assumptions (Shapiro-Wilk's $W<0.96$ $p<0.01$). Hence, the non-parametric alternative to ANOVA called Kruskal-Wallis test was employed to measure and compare the effect of risk communicating cues and privacy priming on app choices. Since, Kruskal-Wallis test cannot be applied to a factorial design, the 4X2 between subject factorial design was transformed to perform one-way non-parametric ANOVA test between 8 experimental conditions: "Control-Primed", "Control-NonPrimed", "Frown-Primed", "Frown-NonPrimed", "Eyes-Primed", "Eyes-NonPrimed", "Lock-Primed" and "Lock-NonPrimed".

Kruskal-Wallis test **on app rating** revealed that there was no significant effect of risk communicating cues and privacy priming on the first app choice across the eight experimental conditions ($\chi^2$ = 11.3, df=7, p = 0.12). A significant effect of risk communicating cues and privacy priming was observed on app rating on the second app choice ($\chi^2$ = 20.9, df=7, p <0.01), third app choice ($\chi^2$ = 83.2, df=7, p<0.01) and fourth app choice ($\chi^2$ = 55.4, df=7, p <0.01). Kruskal-Wallis test **on privacy score** revealed that there was a significant effect of risk communicating cue and privacy priming **on privacy score** on the first app choice ($\chi^2$ = 63.9, df=7, p < 0.01) second app choice ($\chi^2$ = 49.7, df=7, p <0.01), third app choice ($\chi^2$ = 28.7, df=7, p <0.01) and also fourth app choice ($\chi^2$ = 21.9, df=7, p <0.01). Kruskal-Wallis test **on download count** variable revealed that there was no significant effect of cue and priming **on download count** on the first ($\chi^2$ = 1.8, df=7, p= 0.96) and fourth app choices ($\chi^2$ = 4.7, df=7, p=0.68). Although, a significant effect of cue and priming on download count on the second ($\chi^2$ = 15, df=7, p=0.03) and third app choices ($\chi^2$ = 18, df=7, p=0.01) was detected.

Time taken to make app choices was measured. Preliminary analysis showed that participants spent most amount of time in making the first choice which in turn indicated that most of the participants first made all four app choices inside their head and later made actual app installations one by one. Therefore, time taken to make the first choice was considered as indicative of time taken to decide the four app choices. Average time taken to make the first app choice was compared across the eight experimental conditions as show in Figure 5. As it can be seen in Figure 5, irrespective of the type of risk communication cue, participants when primed for privacy spent significantly more amount of time in making app choices (20 seconds more in average).

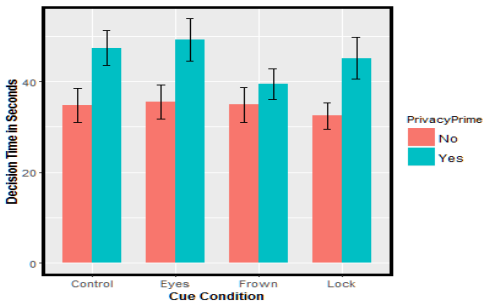


Figure 5: Average time taken to make app choices across the eight experimental conditions

## 5. DISCUSSION

Our work aimed at measuring the effect of privacy priming and risk communicating cues on Android app installation decisions. App choices in Android can widely differ depending on the availability of easy to comprehend risk information early on in the app installation decision process. Participants in the control condition (with no risk communicating cues) made app choices predominantly based on benefits (app rating) while the influence of risk information in the form of install time permissions request was found to be minimal. Consistent with past research, it can be inferred that it is easier for people to rely on app rating to make app choices when it is difficult to assess the risk through privacy permission disclosures. In contrast, when participants were presented with risk communicating cues alongside app ratings, participants were found to choose more number of apps by incorporating both risk and benefits information.

The effect of priming for privacy by itself was found to have less influence on app choices in terms of risk and benefits. As it can be seen in Figure 4, participants in the control condition (with no risk communicating cues), when primed for privacy, made their first choice incorporating both risk and benefits information marginally better than participants who were not primed for privacy. However, the effect of priming was found to deteriorate beyond the first choice. After the first choice, participants in the control condition who were primed for privacy fell back to making choices predominantly based on app rating (benefits) similar to participants who were not primed for privacy. Time taken to make app choices indicated an effect of privacy priming. When participants were primed for privacy, they took significantly more amount of time in making app decisions (20 seconds more in average). It could be theorized that priming for privacy could be leading to increased concern in participants but without appropriate risk communicating cues, people are unable to understand the risk implications of apps, failing to make consistent risk aware app choices.

Overall, framing cues in terms of privacy (positive framing) offered by apps lead to better app choices in comparison to framing in terms of risk to one's privacy. As it can be seen in Figure 3 & Figure 4,

when participants made choices using cues framed in terms of risk (frowny-face and eyes), the first two app choices (while there are more available apps to choose from) were clearly based on both risk and benefits information. However, beyond the first two choices, as the number of available app options reduced, their app choices appears to be inconsistent wherein they neither excel in terms of app rating (benefits) nor in terms of risk rating. In comparison, when participants were presented with cues communicating privacy offered by the apps (using padlocks), decisions on the first two app choices were clearly based on both risk and benefits, similar to app choices made participants using risk framed cues. However, the third and fourth app choices made by participants using privacy framed cues differs from participants using risk framed cues. As it can be seen in Figure 3, we observe a interaction effect of privacy priming in participants in the privacy framed cue condition (padlock condition). Participants using privacy framed cues and who were primed for privacy made the third and fourth choice predominantly based on risk indicating the strong influence of privacy framed risk cues on app choices over other variables such as app rating. However, we do not observe same level of effect in participant using privacy framed cues but were *not* primed for privacy.

Results from this work indicates that cues and scales for communicating privacy risk must be carefully chosen to help users make informed app choices because presenting risk/privacy score in association with other metrics such as app rating could lead to non-intuitive app choices and that different cues and scales can have different degrees of effect on app choices. When people have several good app options available to choose from, we found that any form of privacy risk communication cue or icon (irrespective of framing) will lead to app choices that excel both in terms of risk and benefits. However, when users have to make difficult app choices (when there are only mediocre app options to choose from), both framing of privacy risk cue and individuals' privacy attitude (manipulated through privacy priming) plays a crucial role in app choices. In difficult choice situations, framing cues/icons in terms of privacy offered by the app could lead to more risk averse app choices. Participants who were primed for privacy in the experiment would represent people holding strong concerns towards online privacy and people who have strong concerns towards online privacy would benefit from making app installing decision using visual cues that are framed in terms of privacy offered by the app. Although augmenting concern about one's privacy is not easy as they are largely governed by individual differences and past experiences. One explanation for better performance with privacy framed cues in participants primed for privacy could be that the privacy framed cue was displayed on the same scale as app rating (higher the better) and therefore did not require mental rotations from people for incorporating risk and benefit information in making decisions. It could also be hypothesized that the privacy score was communicated using padlocks which has been found to be representative of user mental models of security [6].

The risk metric used in this experiment was simply based on the number of permissions requested by the app which is clearly not an accurate risk metric but served the purposes of this experiment. There is a significant amount of past work in taint analysis [18, 8, 17, 36, 5] which can analyze Android apps (using Android Application Package) with reasonable accuracy to detect taints in the form of information leaks. It can be argued that outputs from such code analysis tools could be leveraged to develop reliable risk metrics for apps. However presenting risk communicating cues could potentially lead to incorrect sense of safety and mistrust if the methods used for measuring risk is incorrect or simply an approximation. To sustain user trust towards privacy risk communicating cues, it may be beneficial to have a two pronged approach to risk communication in smartphones: (1) present risk communication for apps when the underlying risk assessment is reliable, (2) no risk communication for apps with ambiguous risk assessment allowing people to make better choices atleast based on app ratings and reviews as opposed to misleading them.

We finally conclude by proposing the following five human factor based requirements for designing privacy risk communicating cues based on this work and other past work on risk communication in Android.

1. Privacy communicating icons should be presented early in the decision making process: while people compare apps to choose and install
2. The scale of privacy communicating icons should be consistent with other indicators such as app-rating and download count
3. Privacy communicating icons should be in terms of privacy offered by the app/software
4. Privacy communicating icons should align with user mental models of security
5. Privacy communication should be trustworthy: Risk communication may be avoided when the underlying assessment of an app's privacy risk is ambiguous or inaccurate.

Future research on privacy risk communication needs to further explore the significance of each of these five requirements on people's privacy risk decisions during app installation. Future research is also necessary to identify other crucial human factors based requirements for designing privacy risk communicating cues.

# 6. REFERENCES


[1] Mark S Ackerman and Lorrie Cranor. 1999. Privacy critics: UI components to safeguard users' privacy. In *CHI'99 Extended Abstracts on Human Factors in Computing Systems*. ACM, 258–259.

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[3] Ralph Adolphs. 1999. Social cognition and the human brain. *Trends in cognitive sciences* 3, 12 (1999), 469–479.

[4] Yuvraj Agarwal and Malcolm Hall. 2013. ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*. ACM, 97–110.

[5] Steven Arzt, Siegfried Rasthofer, Christian Fritz, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves Le Traon, Damien Octeau, and Patrick McDaniel. 2014. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. In *ACM SIGPLAN Notices*, Vol. 49. ACM, 259–269.

[6] Farzaneh Asgharpour, Debin Liu, and L Jean Camp. 2007. Mental models of security risks. In *Financial Cryptography and Data Security*. Springer, 367–377.

[7] Kevin Benton, L Jean Camp, and Vaibhav Garg. 2013. Studying the effectiveness of android application permissions requests. In *Pervasive Computing and Communications*

*Workshops (PERCOM Workshops), 2013 IEEE International Conference on*. IEEE, 291–296.

[8] Alastair R Beresford, Andrew Rice, Nicholas Skehin, and Ripduman Sohan. 2011. Mockdroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*. ACM, 49–54.

[9] Rainer Böhme and Jens Grossklags. 2011. The security cost of cheap user interaction. In *Proceedings of the 2011 workshop on New security paradigms workshop*. ACM, 67–82.

[10] José Carlos Brustoloni and Ricardo Villamarín-Salomón. 2007. Improving security decisions with polymorphic and audited dialogs. In *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 76–85.

[11] Jing Chen, Christopher S Gates, Ninghui Li, and Robert W Proctor. 2015. Influence of risk/safety information framing on android app-installation decisions. *Journal of Cognitive Engineering and Decision Making* 9, 2 (2015), 149–168.

[12] Pern Hui Chia, Yusuke Yamamoto, and N Asokan. 2012. 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*. ACM, 311–320.

[13] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. 2013. Nudging people away from privacy-invasive mobile apps through visual framing. In *Human-Computer Interaction–INTERACT 2013*. Springer, 74–91.

[14] Vincent C Conzola and Michael S Wogalter. 2001. A communication–human information processing (C–HIP) approach to warning effectiveness in the workplace. *Journal of Risk Research* 4, 4 (2001), 309–322.

[15] Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. 2011. PiOS: Detecting Privacy Leaks in iOS Applications.. In *NDSS*.

[16] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1065–1074.

[17] William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N Sheth. 2014. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)* 32, 2 (2014), 5.

[18] William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri. 2011. A Study of Android Application Security.. In *USENIX security symposium*, Vol. 2. 2.

[19] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 3.

[20] Vaibhav Garg and Jean Camp. 2012. End user perception of online risk under uncertainty. In *System Science (HICSS), 2012 45th Hawaii International Conference on*. IEEE, 3278–3287.

[21] Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM, 71–80.

[22] Jens Grossklags and Alessandro Acquisti. 2007. When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information.. In *WEIS*.

[23] M Hettig, E Kiss, JF Kassel, S Weber, M Harbach, and M Smith. 2013. Visualizing Risk by Example: Demonstrating Threats Arising From Android Apps. In *Symposium on Usable Privacy and Security (SOUPS)*.

[24] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3393–3402.

[25] Swapna Kolimi, Feng Zhu, and Sandra Carpenter. 2012. Contexts and sharing/not sharing private information. In *Proceedings of the 50th Annual Southeast Regional Conference*. ACM, 292–297.

[26] David Kravets. 2014. Spyware executive arrested, allegedly marketed mobile app for' 'stalkers". In *arstechnica*. 279–298.

[27] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15, 4 (2004), 336–355.

[28] Alexios Mylonas, Anastasia Kastania, and Dimitris Gritzalis. 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security* 34 (2013), 47–66.

[29] Helen Nissenbaum. 1998. Protecting privacy in an information age: The problem of privacy in public. *Law and philosophy* 17, 5 (1998), 559–596.

[30] Henry L Roediger and Jeffrey D Karpicke. 2006. The power of testing memory: Basic research and implications for educational practice. *Perspectives on Psychological Science* 1, 3 (2006), 181–210.

[31] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 1–17.

[32] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness.. In *USENIX Security Symposium*. 399–416.

[33] Jeff Sweat. 2000. Privacy paradox: Customers want control–and coupons. *Informationweek* 781, April (2000), 52.

[34] Amos Tversky and Daniel Kahneman. 1992. Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and uncertainty* 5, 4 (1992), 297–323.

[35] Haidong Xia and José Carlos Brustoloni. 2005. Hardening web browsers against man-in-the-middle and eavesdropping attacks. In *Proceedings of the 14th international conference on World Wide Web*. ACM, 489–498.

[36] Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and Vincent W Freeh. 2011. Taming information-stealing smartphone applications (on android). In *Trust and Trustworthy Computing*. Springer, 93–107.