Interaction Effects of Contextual Cues on Privacy Concerns: the Case of Android Applications

Jie Gu
Fudan University,
Shanghai China
gjtracy20@gmail.com

YunJie Xu
Fudan University,
Shanghai China
yunjiexu@fudan.edu.cn

Heng Xu
Pennsylvania State University
hxu@ist.psu.edu

Hong Ling
Fudan University,
Shanghai China
hling@fudan.edu.cn

Abstract

The prevalence of mobile applications poses a new challenge in privacy protection. To address privacy concerns, prior studies have identified the direct effects of contextual cues but few have revealed their interaction effects. In reality, contextual cues do not appear in isolation; existence of multiple contextual cues introduces an extra complexity in a user’s privacy decision-making. This study aims to address the research question of how contextual cues interactively shape privacy concerns. This study focuses on the Android application downloading context. Three contextual cues (i.e., app popularity, permission sensitivity, permission explanation) are identified. Our experimental study postulates both the direct effect and interaction effects of contextual cues on privacy concerns. This study contributes to literature with a better understanding of the combinatory effects of multiple contextual cues.

1. Introduction

Information privacy has attracted ever-growing attention in today’s technology-based environment [26]. The prevalence of mobile applications poses a new challenge in privacy protection [37]. Third-party applications installed on smartphones have an easy access to a large amount of personal data and on-device resources in real time [37]. Mobile malware has been reported to grow 614% in one year from March 2012 to March 2013 [16]. A 2013 research report stated that Android is responsible for 92% of all known mobile malwares [16].

Recent privacy research has increasingly focused on identifying the antecedents of context-specific privacy concerns [35]. Emphasizing the role of context-specific privacy concerns, researchers identified contextual cues that affect people’s privacy decision making [1, 3, 12, 14, 15, 21]. For example, previous studies have examined the direct effect of sensitivity of information request [1, 12, 21], explanation of privacy items [14, 15, 17] and a variety of social cues [3, 12] in assisting people to make informed privacy decisions. However, prior research limited their attention on the individually direct effects of these cues. In reality, contextual cues do not appear in isolation. Existence of multiple contextual cues introduces an extra complexity.

This study focuses on the interaction effects of multiple contextual cues. Particularly, this study investigates how contextual cues interactively shape Android users’ privacy concerns in the context of application downloading. We argue that Android application downloading phase warrants attention because it is the first step against inappropriate data collection and misuse. Three typical contextual cues are addressed in our experimental study. They are application popularity, permission request, and permission explanation. Popularity is an indicator of the choices made by early adopters [11]. It refers to what is widely accepted or liked by others. In the context of Android application downloading, application popularity is usually presented by the number of downloads. Application developers have to request permission to enable applications to realize their functions [1]. Permission requests usually involve applications’ access to and use of on-device privacy information [10]. There are a few Android markets that have disclosed developers’ permission request before users download their applications. Application popularity and permission request are observable in current Android application downloading webpage. This study introduces a new contextual cue, permission explanation, into the Android application downloading
context, and investigates its design and impact. Permission explanation refers to a statement of what information is collected, how users’ information is used and who can get access to the on-device information and resources. Permission explanation helps justify an application’s requests for permissions, hence makes these permissions more relevant to the function of an app. This study expects that contextual cues interactively influence users’ relevance perception, which further affect their privacy concerns.

This study contributes to the privacy literature by exploring the interaction effects of contextual cues. Conclusion of this study reveals that the effectiveness of some contextual cues depend on the level of others when they are used in combination. From the practical perspective, our findings suggest Android practitioners to leverage contextual cues to inform users of their privacy practices. This study suggests the importance of an in-depth investigation on the effectiveness of multiple privacy cues when they are used in combination.

2. Literature review

2.1. Role of perceived relevance

Researchers have argued that information privacy is one of the most important topics in today’s networked world [23, 28, 34]. Personal information in a digital format can be easily collected, copied and transmitted, which enables other parties to construct opportunistic behavior more easily [21]. Privacy invasion poses serious threats to information security [36].

It has been posited that individuals tend to have a lower level of privacy concerns if they perceive a high degree of fairness over the collection and use of their personal data [6]. In consumer marketing, consumers’ fairness perceptions on whether their information is collected and used fairly play an important role in predicting their information disclosure behaviors [6]. When consumers are informed about a firm’s information practices and perceive the business as fair to them, they are more willing to disclose personal information [5]. Previous research on online social application has revealed that people desired to share information only when it was necessary for an application to function [2].

To capture individuals’ fairness perceptions in information exchange, Li et al. introduced the notion of perceived relevance over firms’ information requests [19]. Perceived relevance captures an individual’s perception of whether an information request is relevant to the purpose of transaction [5]. A few privacy studies have examined the role of perceived relevance in predicting information privacy concerns. For example, in an experimental study, Li et al. proposed that perceived relevance helps to mitigate individuals’ privacy risk perceptions [19]. In addition, Wang et al. found that perceived relevance alleviates privacy concerns towards mobile advertisement [33].

2.2. Effects of contextual cues

Recent privacy research has focused on context-specific privacy concerns. Context has been defined as “stimuli and phenomena that surround and exist in the environment external to the individual” [35]. By focusing on context-specific privacy concerns, researchers investigated the effects of contextual cues in influencing individuals’ privacy decision making.

The privacy literature has investigated various contextual cues that are able to signal information privacy. These cues include a variety of visualization icons which aim at enhancing individuals’ privacy awareness [17, 30, 32], and the form of information presentation which navigates individuals through privacy list more efficiently [14, 15, 17]. Recently, research has increasingly focused on contextual cues that assist users to make more informed privacy decisions. These cues include sensitivity of information request [1, 12, 21], explanation of privacy items [14, 15, 17] and the emergent effects of social cues [3, 12].

One of the most primary cues in privacy decision making is information sensitivity [9, 21]. In ecommerce, the request of financial data and medical information is viewed as sensitivity cue [21]. In the domain of third-party application, the number of permissions and the sensitivity of the requested items were both considered as cues to signal the level of information sensitivity [12]. Despite of different sensitive cues in different contexts, a common view is that an individual has a higher level of privacy concerns when he or she notices a sensitivity cue [20, 21, 24].

The ineffectiveness of privacy policies in warning against privacy threats has been a big concern for both researchers and practitioners. Good et al. found that the regular end-user license agreement (EULA) was too long for users to read and the use of technical terms was hard for general users to understand [14]. In hoping to remedy this issue, a few researchers have discussed the effect of a concise explanation of the purpose, storage
and access of personal information in software installation [14, 15, 17]. More specifically, explanation refers to a statement about what information is collected, how personal information is used and who can get access to collected information. Good et al. designed an experiment to incorporate a short notice with such an explanation on a software installation page. Results indicated that the presence of the explanation reduced installations of bundled spywares [15]. In a follow-up study, they offered users with either a pre-installation or a post-installation notice explaining the potential privacy-intrusion actions of the given software. They found that a pre-installation notice with a privacy explanation reduced the number of spyware installations, while a post-installation privacy explanation led to a significant number of uninstalls [14]. Kelley et al. found that website users felt better informed when they were provided with an explanation of website privacy policy [17]. While the above research has proposed the effects of explanation, few explored individuals’ perception response to privacy explanation.

Recent research has revealed that social cues, such as the number of users, significantly affect individuals’ privacy decision making [24]. Individuals tend to infer a lower level of privacy threat if they notice that many others have adopted the same application. Besmer and Lipford suggested that the presence of social cues affect users’ decisions in access control settings for social applications. They found that users were less likely to opt out a permission request if many others approved its access [3]. Similarly, Eling et al. indicated that the number of users can have a positive effect on users’ trust beliefs towards an unknown social application [12]. Although social cues have been criticized by the possible herding consequence and adverse selection results, user studies have confirmed the critical effects of social cues in influencing mobile users’ privacy decision making [3, 18].

While there are a few contextual cues which assist individuals to make privacy decision, the purpose of this research is not to perform a comprehensive examination of all contextual cues related to context-specific privacy concerns. Rather, we focus on three types of contextual cues (i.e., sensitivity, explanation, popularity) and examine their interaction effects. An interesting question here is that even if an array of contextual cues are each demonstrably effective, it is not clear how effective they will be when used in combination [4].

3. Hypotheses development

This study investigates users’ privacy concerns in the context of downloading Android application. Users genuinely want to protect privacy in application downloading process as it is the first step against information over-collection and misuse. The 2013 U.S. Consumer Confidence Index reveals that 81% of smartphone users avoided applications that were believed to threaten their privacy [29].

This study focuses on three contextual cues that could appear on an Android application’s downloading page: application popularity, permission request, and explanation for requested permissions. We choose these three cues as they provide users with privacy-relevant cues to make better informed decisions. Among them, popularity is a typical social cue in application market. It is usually presented by the number of downloads. A few application markets (e.g., www.mumayi.com) choose to disclose the permission request of published applications as a way to show their respect for users’ privacy. Permission request can be of either high or low sensitivity based on the number and type of permissions requested. Explanation is a contextual cue designed by this study. Although it is not new in the domain of website privacy policy or software installation, the current Android market has not incorporated permission explanation into the application presentation. A non-technical explanation of a permission request helps users to comprehend the permission request. More specifically, we expect that explanation can mitigate privacy concerns by boosting the relevance perception of requested permissions. By emphasizing these three contextual cues, we are not only interested in their direct effects, but also their interaction effects in shaping privacy concerns via the cognitive mechanism of perceived relevance. The research model of this study is illustrated in Figure 1.
3.1. Antecedents of privacy concerns

In the mobile context, perceived relevance is defined as the extent to which a permission request is relevant to an application’s core function. When individuals perceive a high relevance, they are less likely to worry about their privacy [19, 33]. Relevance perception is sensitive to the specific context. Imagining that both a console game and a map application request for location information, the location request should be more relevant in the context of the map application than that of mobile game. The mobile game application’s permission request for location information would trigger users’ privacy concerns because location is less relevant with its core function and therefore seems unreasonable. Thus we hypothesize:

Hypothesis 1 (H1). The perceived relevance of an application’s permission request has a negative effect on the context-specific privacy concerns of the mobile application.

Information sensitivity is viewed as a primary contextual variable in the literature [21]. Research has suggested that highly sensitive information exerts a positive effect on an individual’s privacy concerns [20, 21, 24].

Android operating system defines app permissions into different types according to threat levels [1]. For example, permissions such as “access to the vibrator” and “keeping device screen awake” are considered as of minimal risk. However, “access to location information” and “access to contact information” are considered as highly sensitive and could pose a threat to the user’s privacy. Sensitivity of permissions may arise from both the number of permissions requested [31] and the severity of possible negative consequences [5]. Highly sensitive permissions are perceived to be more risky [21], which activate privacy concerns more easily [7, 8]. Thus we hypothesize:

Hypothesis 2 (H2). Permission sensitivity has a positive effect on the context-specific privacy concerns.

When users are not familiar with an application, they tend to believe that a highly popular application is less likely to have privacy threats [18]. While application popularity itself does not say anything about the privacy practice of the application, it can be regarded as a cue to mitigate privacy concerns. High popularity indicates that lots of prior adopters have made their downloading decisions. When many others are involved in using the same application, a user’s perceived uncertainty of the possible privacy threat is reduced. Such positive perception induced by popularity cue also mitigates privacy concerns by reducing users’ motivations to process inconsistent negative information related to privacy concerns. Therefore we hypothesize:

Hypothesis 3 (H3). Application popularity has a negative effect on the context-specific privacy concerns.

3.2. Effects of contextual cues on perceived relevance

Another contextual cue addressed in this study is the non-technical explanation for permission requests. At this stage, no Android application market has incorporated permission explanation in their application presentation. However, prior literature has suggested that explicating the purpose of information collection is an effective way to ease privacy concerns [18, 27]. In this study, we define explanation as a

---Not specifically hypothesized but path included for statistical testing

Figure 1 Research model
statement of the purpose and access of collected information. This definition is in alignment with the “Notice” principle addressed by the Fair Information Privacy Principles (FIPP). The key objective of FIPP is to assure that privacy practices are fair [27]. The “Notice” principle, which refers to the disclosure of what information is collected, by whom and for what purpose, is thus intended to justify the fairness of information practice and hence result in an increase in individuals’ relevance perceptions. Following this argument, we propose that permission explanation should reduce privacy concerns via improving relevance perception. Particularly, a clear explanation of data collection purpose makes users believe that the collected information is relevant to the functioning of the application.

**Hypothesis 4 (H4). Users will perceived higher relevance of the permission request when they are provided with permission explanation**

While an explanation can directly enhance perceived relevance, we postulate application popularity and permission sensitivity as moderators of explanation. As these contextual cues do not appear in isolation in practice, their interaction effects are more appealing.

First, we regard permission sensitivity as a necessary condition for explanation to operate on perceived relevance. If an application only requests insensitive permissions which are considered as “safe” for users, users are likely to dismiss the content of explanation. In this circumstance, users are likely to follow such a heuristic evaluation rule over multiple contextual cues: when permission sensitivity is low, explanation loses its value in enhancing perceived relevance. Users would read explanation for clarification only if the permission request is sensitive enough to catch users’ attention. Thus we hypothesize:

**Hypothesis 5 (H5). Permission sensitivity positively moderates the effect of explanation on the perceived relevance of permission request.**

Second, we argue that popularity enhances the effect of explanation. Explanation boosts perceived relevance only when it is considered as trustworthy. Because the explanation is provided by the application, users may doubt about the truthfulness of the explanation. High popularity indicates that the specific application has been evaluated and approved by many others. Literature has proven that the number of users can have a positive effect on users’ trust towards application-relevant information, i.e., permission explanation in our case. Because of the absence of official guarantees of the trustworthiness of explanation, others’ behavior acts as a “trust” reference. This study argues that popularity amplifies the effect of explanation by referring explanation trustworthiness.

**Hypothesis 6 (H6). Application popularity positively moderates the effects of explanation on perceived relevance of permission request.**

Prior privacy research suggests additional factors should be included as control variables because of their potential influence on our dependent variable. Because our primary theoretical focus is not on them, we include them as control variables to eliminate the variance explained by them. They are gender [22] and general privacy concerns [21].

### 4. Methodology and data analysis

#### 4.1. Experiment design

A scenario-based experiment was designed to collect data. Subjects were assumed to download a given app from an unfamiliar Android application market named “Android App World”. We did not use the name of an established Android market in order to control for extraneous market influence. The design of the experimental page was adapted from a real Android market (mumayi.com) to enhance the mundane reality. Participants first read the information of an app named “Delicacy”. The core function of “Delicacy” was to provide restaurant descriptions and customer reviews. “Android App World” and “Delicacy” were both coined by researchers to make sure that participants had no prior experience with them. After reading the page, subjects were asked to fill out a questionnaire.

Eight experimental scenarios were designs based on a 2 (high or low popularity of the given app) × 2 (high or low sensitivity of app permissions) × 2 (with or without explanation for permissions) combination. Participants were randomly assigned to one of the eight scenarios. Manipulations of the three contextual cues were listed as follows:

**Popularity cue** was manipulated by the position of Delicacy in a monthly downloads ranking list. High popularity was manipulated as the 1st rank with most downloads, whereas low popularity was manipulated as the 40th at the bottom of a page.

**Permission sensitivity** can be caused by both the
number of permission requests and the severity of negative consequences. In the low-sensitivity group, the application required only an access to the vibrator and keeping device screen awake. In the high–sensitivity group, the application required access to location information and access to contact list, in addition to the two permissions in the low sensitivity group.

Explanation was manipulated by the presence or absence of a non-technical explanation for each application permission request. In the “with-explanation” group, subjects were presented with the purpose of each permission request, and were assured that the information collected (if any) will not be transferred to a server. Corresponding explanations for permissions involved in this study were listed as follows:

1. Explanation for “access to the vibrator”-- Remind users when there is a new announcement.
2. Explanation for “keeping device screen awake”--Prevent the running application from being interrupted when the device turns into a sleeping mode.
3. Explanation for “access to GPS location”--Provide personalized recommendations of local restaurants. Users’ location will not be disclosed to any third party.
4. Explanation for “access to contact list”-- Enable Delicacy’s social network function: share your experiences with friends anytime and anywhere. User’s contact list will not be disclosed to any third party.

4.2. Instrument development and validation

Existing scales of latent constructs were adapted to fit the study context. Items for perceived relevance were adapted from Li et al.[19]. The instrument for general privacy concerns was based on items developed by Malhotra et al. [21]. Users’ context-specific privacy concerns were adapted from Smith et al. [25].

The survey instrument was pretested in two phases: (1) a face-face interview with a convenience sample to ensure face validity, and (2) an online pilot study with student samples. In the first phase, participants were asked to identify confusing items. In the pilot study, 94 Android users successfully completed an online survey. The pilot survey data was used to check the validity of our manipulations on contextual cues and to verify psychometric qualities of the scales. We adjusted or dropped those items which did not pass our exploratory factor analysis.

College students from a major university in Shanghai, China served as participants for this study. None of them participated in the pilot study. A total of 286 participants were invited and 265 of them completed the survey. Non-response bias was checked by comparing incomplete responses with complete ones. No systematic differences were identified regarding gender or general privacy concerns. In the 265 completed responses, 170 were identified as Android users and 95 were not. We restricted our data analysis to only Android users.

In order to ensure that our manipulations produced desired effects, we did manipulation check before testing hypotheses. Several questions asked participants about their perceived popularity and sensitivity in the questionnaire. One-way analysis of variance (ANOVA) was used to test the effectiveness of two contextual cues on popularity and sensitivity. For perceived popularity, the application at the top of the 1st was perceived more popular than the one at 40th (p<0.001). Participants in the high-sensitive group perceived higher sensitivity regarding permission request (p<0.001) than those in the low-sensitive group. To confirm participants’ awareness levels of explanations, explanations were highlighted and participants were asked to line up the permissions with their corresponding explanations. We dropped 5 participants who failed all line-up questions. Finally, we had 165 respondents in our data analysis. Among the 165 respondents, there were 68 males (41.2%) and 97 females (58.8%).

We first tested the measurement model. The convergent validity of the measurement model was satisfactory, with (1) all item loadings exceeding 0.65, (2) Cronbach’s alpha greater than 0.70, (3) and the average variance extracted (AVE) for each construct greater than 0.50. The discriminant validity was also satisfactory, with the square roots of the AVEs greater than the correlations between constructs.
4.3. Hypotheses testing

Research hypotheses were tested by partial least squares (PLS). We estimated two models using PLS. Model 1 is our research model, whereas Model 2 is a reduced model that contextual cues directly lead to privacy concerns without perceived relevance. Model fitting results were presented in Figure 2a and Figure 2b.

Results in Model 1 indicated a significantly negative effect of perceived relevance on contextual-specific privacy concerns (beta=-0.266, p<0.01). H1 is thus supported. We also found a significantly positive effect of sensitivity on privacy concerns (beta=0.299, p<0.01). Thus H2 is supported. However, the hypothesized negative effect of popularity on privacy concerns was only weakly significant at p<0.1 level. Regarding the effect of contextual cues on perceived relevance, the main effects of explanation was not significant, thus H4 was not supported. The interaction term SEN*EXP was positively significant (beta=0.271, p<0.01), demonstrating support for H5. The interaction term POP*EXP was also significant with expected positive effect (beta=0.269, p<0.01), thus H6 was supported. From these results we concluded that permission explanation alone could not mitigate privacy concerns through increasing relevance perception in a consistent way. In fact, the effect of explanation was
highly dependent on the levels of application popularity and permission sensitivity.

To highlight the cognitive effect of perceived relevance in influencing privacy concerns, we also estimated a reduced model in which contextual cues directly lead to privacy concerns without perceived relevance. R-square for privacy concerns in Model 2 was 22.1%. R-square of the direct effect model and our research model indicated an incremental variance of 6.6% (28.7%-22.1%). This suggests that perceived relevance is a cognitive mechanism influencing privacy concerns in Android application downloading context.

5. Discussion and contribution

This work revealed some interesting results. First, a user’s privacy concerns are positively affected by the user's perception of permission sensitivity. Meanwhile, popular application is believed to be less privacy-threatening. However, the negative effect of popularity on privacy concerns was relatively weak supported at the level of $p<0.1$. Besmer et al. indicated that the number of prior users did have an impact in privacy decision-making, but only with strong visualization cues [3]. Thus one plausible explanation for this relatively weak effect of popularity cue on privacy concerns is that our visual design of popularity was not strong enough. We also found that perceived relevance of permission request eased privacy concerns. This result provides an insight on how context-specific privacy concerns can be alleviated by raising users’ relevance perceptions over permission request.

Permission explanation is expected to serve as an effective approach to enhance perceived relevance. In the experiment, by clarifying the purpose and data policy for each permission request, users were supposed to easily link permission request to the application function, thus perceived a higher level of relevance. Surprisingly, we found that offering permission explanation alone did not increase users’ relevance perceptions in a consistent way. Instead, the effect of explanation was highly dependent on the levels of other contextual cues. The interaction effects among contextual cues demonstrated in PLS were confirmed by ANOVA. The main effect of explanation was still insignificant. There was a significant interaction between popularity and explanation ($F=3.931$, $p<0.05$) and between sensitivity and explanation ($F=4.409$, $p<0.05$). Both PLS and ANOVA results have revealed that when an application was unpopular and with low privacy sensitivity, explanation had no effects on perceived relevance. In contrast, explanations boost perceived relevance for a popular application. Also, highly-sensitive permission request triggered the effects of explanation in a significant way.

We extend the literature with a better understanding on the combinatory effects of multiple contextual cues. While a few contextual cues have been investigated in prior studies, the interaction effects of these contextual cues are under-explored. Prior research on contextual cues has primarily focus on how these cues individually influence privacy-related constructs. However, when there are a few cues present to users, how effective they will be is still a question. Findings of this study suggest that the effects of some cues do depend on the levels of others. This study contributes to privacy research by suggesting an in-depth investigation over the combinatory effects of contextual cues when they coexist in an individual’s privacy decision-making process.

In addition to our theoretical contribution, our research provides implications for practitioners. First, considering the effects of popularity, Android markets are suggested to highlight application popularity to help a user’s privacy decision-making. Secondly, we suggest Android markets to ask developers to present permission request for each application. For non-technical users, their perceived permission sensitivity for each permission request will warn them about potential risks before they download suspicious apps. For developers, this disclosure practice motivates them to only request for necessarily minimum amount of permissions. Thirdly, we suggest Android markets to take an effort to provide a concise explanation for the purpose, and usage of permission requests. This kind of non-technical explanation helps general users to better comprehend permission requests. Android applications normally require more permissions than they need [13, 32]. If developers are asked to describe the purpose of each permission request, they will have to restrict their permission requests to the minimum. In this sense, explanation designed by this study would help to build a “self-regulated” Android application ecosystem. Finally, the interaction among explanation and other contextual cues also make practitioners to pay attention to their combinatory effects. Even when an Android market provides permission explanation for applications published onto it, the presence of explanation does not equally benefit all applications.
6. Limitation and conclusion

Our study has several limitations. The scenario-based experiment employed only one specific type of smartphone application. In the future, we plan to repeat this study in other types of applications because specific features of app functions are expected to raise different levels of privacy concerns. To imitate the real app downloading process, especially through on-device app store, a more vivid app downloading scenario is a necessity in our future study.

In summary, this study seeks to explore the interaction effects among contextual cues on context-specific privacy concerns. In the process of downloading Android application, we investigated three contextual cues: permission sensitivity, application popularity and permission explanation. We chose these three cues as they are suggested to help users to make a better informed privacy decision [1, 3, 12, 14, 15, 21] and can be easily presented in the application description page. An interesting question here is that even if each of these contextual cues could be effective, it is not clear how effective they will be when used in combination [4]. We proposed that the interaction effects among these three contextual cues work through perceived relevance over permission request. In general, the results supported our core assertion that these cues interactively shape users’ privacy concerns through the cognitive mechanism of relevance perception.

7. References: