Received: 6 November 2017 | Revised: 23 April 2018 | Accepted: 1 August 2018

DOI: 10.4218/etrij.2017-0259

ORIGINAL ARTICLE

WILEY ETRI Journal

How do multilevel privacy controls affect utility-privacy trade-offs when used in mobile applications?

Seung-Hyun Kim[1] | In-Young Ko[2]

[1]Hyper-connected Communication Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea.

[2]School of Computing, Korea Advanced Institute of Science and Technology, Daejeon, Rep. of Korea.

Correspondence
Seung-Hyun Kim, Hyper-connected Communication Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea.
Email: ayo@etri.re.kr

Funding information
Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2016-0-00097, Development of Biometrics-based Key Infrastructure Technology for On-line Identification). This work was also supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2016R1A2B4007585).

In existing mobile computing environments, users need to choose between their privacy and the services that they can receive from an application. However, existing mobile platforms do not allow users to perform such trade-offs in a fine-grained manner. In this study, we investigate whether users can effectively make utility-privacy trade-offs when they are provided with a multilevel privacy control method that allows them to recognize the different quality of service that they will receive from an application by limiting the disclosure of their private information in multiple levels. We designed a research model to observe users' utility-privacy trade-offs in accordance with the privacy control methods and other factors such as the trustworthiness of an application, quality level of private information, and users' privacy preferences. We conducted a user survey with 516 participants and found that, compared with the existing binary privacy controls, both the service utility and the privacy protection levels were significantly increased when the users used the multilevel privacy control method.

KEYWORDS
fine-grained privacy controls, mobile computing environments, multilevel privacy controls, quality of private information, utility-privacy trade-offs

1 | INTRODUCTION

Mobile applications utilize users' private information to provide personalized services to users. However, there are many mobile applications that cause privacy infringement problems by excessively accessing users' private information that is not necessary to provide to their services. Some users, who are seriously concerned about privacy infringement, avoid installing and using such mobile applications [1]. However, some users place more weight on the service utility that they can receive from an application and ignore the potential privacy infringement problems that might be caused by the application [2]. According to the privacy calculus theory, users' privacy decisions on disclosing their private information are made by making a trade-off between utility and privacy [3].

However, existing mobile platforms do not allow users to perform such precise trade-offs. Although most of the existing mobile platforms provide functions for managing permissions to access users' private information, users can employ merely binary privacy controls while submitting their private information to mobile applications. In other words, in response to an application's request to access a user's private information, the user can either “allow” or “deny” the access to the private information. In addition, under the current mobile platforms, users are provided with very limited information to make efficient privacy decisions. For example, the latest mobile operating systems from Google and Apple allow users to check only the types of private information to be sent to an application. Therefore, in many cases, users cannot effectively understand the application's purpose of using the private information.

There have been few studies done on providing fine-grained privacy controls to users in mobile computing environments. Although there are some studies that proposed multilevel privacy control methods, they focused mostly on the technical issues of making mobile applications to deal with multilevel private information. To the best of our knowledge, there have been no systematic studies on checking the effectiveness of using multilevel privacy controls in terms of maximizing users' utility of mobile applications and minimizing the quality and quantity of private information to be transmitted to the applications.

The main purpose of our study was to present empirical evidence of the effectiveness of using multilevel privacy controls in mobile computing environments. In this study, we investigate whether users can effectively make utility-privacy trade-offs when they are provided with a multilevel privacy control method that allows them to recognize the different quality of service (QoS) that they will receive from an application by limiting the disclosure of their private information in multiple levels. To investigate this, we defined the following research questions:

> *RQ1:* Can users make more efficient utility-privacy trade-offs by using multilevel privacy controls compared with using existing binary privacy controls?
>
> *RQ2:* How do privacy-related factors such as the trustworthiness of an application, the quality level of private information, and the users' privacy preferences that are known to affect users' utility-privacy trade-offs influence users' multilevel privacy controls?

To answer these research questions, we conducted a user survey with 516 participants. In the survey, the participants were asked to make privacy decisions in practical usage scenarios of mobile applications. The usage scenarios were based on different situations involving the use of mobile applications, such as different trustworthiness of the applications, and various levels of private information to be provided to the applications. To make the participants consider the practical situations of using mobile applications, we allowed users to choose mobile applications that they are familiar with. In addition, by applying the privacy-related factors that have been identified in related studies, we could find that all the privacy-related factors significantly affect the multilevel privacy controls at the point of users' privacy controls.

The rest of this paper is organized as follows. In Section 2, we explain the theoretical background and hypotheses about the relationship between multilevel privacy controls and users' utility-privacy trade-offs. In Section 3, we describe the design of our user survey and its procedure. In Section 4, we present and analyze the results of the user survey by using a statistical method. We discuss the analysis results and the issues with the validity of the results in Section 5. In Section 6, we explain existing work on modeling and analyzing users' privacy decisions, and discuss how our analysis goal and approach are different from them. Finally, in Section 7, we conclude the paper and discuss future works.

2 | BACKGROUND AND HYPOTHESES

2.1 | Utility-privacy trade-offs

A *utility-privacy trade-off* refers to the behavior of users when choosing between the perceived service utility of an application and their privacy protection when deciding on whether to provide private information to the application [4]. Understanding these trade-off behaviors of users is essential not only for users but also for service providers. Service providers usually collect users' private information to provide personalized services that can satisfy users' expectations [5].

A number of studies have been performed to analyze the mechanism of utility-privacy trade-offs made by users. A representative concept of the utility-privacy trade-off is called the *privacy calculus theory*. This concept frames users' disclosure of private information as a trade-off between the service utility and the privacy risks [6]. The majority of related studies simply assumed that the service utility is inversely related to the privacy risk and presented various mathematical models to express utility-privacy trade-offs. However, some studies observed users' utility-privacy trade-offs made in practical situations and analyzed the relationship between the users' privacy decisions and various factors such as the trustworthiness of service providers, the quality level of private information to be sent to the service providers, and the users' privacy preferences [7]. They found that these privacy-related factors significantly influence the users' privacy decisions.

2.2 | Multilevel privacy controls

Kim et al. defined various types and quality levels of private information in an ontology-based model called the quality of private information (QoPI) model [8]. A QoPI level defines the quality of private information that can be sent to a mobile application by modifying the original private information to a form that meets a user's privacy requirement. A QoPI modification method indicates the method that can be employed for modifying users' private information into a required abstraction level (ie, a QoPI level). The QoPI model can represent 17 types of contextual properties in four contextual aspects that might affect users' privacy decisions.

As explained in the study, the multilevel privacy control method allows users to provide their private information by modifying its quality at a certain level that they want. To do that, it is necessary to define multiple quality levels of private information and the modification methods that modify the original private information according to the quality level selected by a user. In the previous study, they conducted an intensive survey on existing approaches to represent multiple abstraction levels of private information, and defined a model to represent five different quality levels of private information (from "no disclosure of private information" (Level 0) to "full disclosure of private information" (Level 4)) that can be applied to various types of private information in the mobile computing domain.

Figure 1 shows the QoPI model that they proposed in their previous work [8]. The parts that are highlighted with a red box are for specifying the QoPI levels and the modification methods. The "Original Private Information" indicates the users' original private information. The "Modified Private Information" is the users' private information that is modified into a certain quality. The "QoPI Level" specifies the quality of private information that is to be provided to a service provider. The "Modification Method" specifies a modification method to be used to modify the original private information according to a QoPI level.

Although the previous study of Kim et al. showed that users prefer to use the multilevel privacy control method than the binary privacy control method, there is room for further research. First, it is necessary to understand how different privacy control methods affect users' privacy decisions in a given situation. Second, it is necessary to analyze what privacy-related factors affect users' privacy decisions when they use multilevel privacy controls.

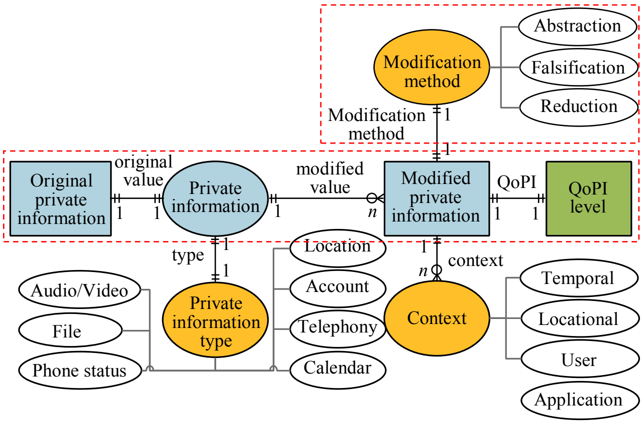


FIGURE 1 QoPI ontology model [8]

2.3 | Hypotheses on privacy-related factors

2.3.1 | Privacy control methods

The presence of an efficient privacy control method helps users to reduce their perceived privacy risks. Milne and Boza showed that users' privacy concerns are reduced when they feel they can control their private information [9]. Chellappa and Sin also found that, regardless of the quality level of private information, those who can control their private information usually want to provide more private information to service providers compared with users who do not have such control [10]. Based on these findings, we can assume that compared with the binary privacy control method, the multilevel privacy control method will make users be more protective in providing their private information (H1), while still allowing mobile applications to access greater amounts of their private information, but of lower quality (H2).

2.3.2 | Trustworthiness of applications

The trustworthiness of an application is one of the main criteria that users consider when choosing a service provider. Existing studies define the trustworthiness of an application as the basis of the quality of personalized services that it provides [11]. Kehr et al. also found that the trustworthiness of a smartphone application affects users' perceived service utility of the application [12].

Users' privacy concerns with a service provider are usually reduced if they trust the service provider. Milne and Boza showed that building trust from users by a service provider is crucial to reduce users' privacy concerns with the service provider [9]. Because of this, the trustworthiness of a service provider affects users' privacy controls and their intention of providing private information [2].

When using the multilevel privacy control method, compared with the binary privacy control method, users will make moderate privacy decisions by choosing an appropriate quality level of privacy information on the basis of the trustworthiness of a mobile application. Therefore, we hypothesize that users will protect their privacy even for trustworthy mobile applications when they have multilevel options to provide private information to the applications (H3). In addition, users will utilize some of the services that are provided by untrustworthy applications when they can limit the amount and quality of private information to be sent to the applications (H4).

2.3.3 | Quality level of private information

Several studies showed that the quality level of private information is an important factor that greatly affects users' privacy decisions [13,14]. The reason for this is that providing high-quality private information to an application is considered as a high risk of privacy exposure [15]. The quality level of private information also affects the expected service utility from an application. Users usually expect more service utility when they provide high-quality private information to an application [16].

When users are presented with the multilevel privacy control method, compared with the binary privacy control method, they can modify the high-quality level of private information to a certain abstract level such that their privacy can be protected while achieving a certain level of service utility. Therefore, we hypothesize that users will utilize some services from mobile applications that require high-quality private information when they can modify this information by using the multilevel privacy control method (H5). In addition, even if a mobile application asks for low-quality private information, users can still try to protect their privacy by further limiting the amount and quality of private information (H6).

2.3.3 | Privacy preferences

Many studies showed that users' general tendency toward privacy (privacy preference) affects the disclosure of their private information [13,14,17]. Knijnenburg and Kobsa showed that users with a positive privacy preference (optimistic users) disclose more of their private information while trying to increase the perceived service utility [18]. However, users with a negative privacy preference (pessimistic users) usually have high privacy concerns [17] and limit the disclosure of their private information [19]. Therefore, pessimistic users usually do not try to increase the perceived service utility by providing more private information [17].

Compared with the case of using the binary privacy control method, by using the multilevel privacy control method, users can control both the degree of privacy protection and the level of service utility when making moderate privacy decisions based on their privacy preferences. Therefore, we hypothesize that users who have a positive privacy preference will use more privacy protection when they use the multilevel privacy control method (H7). On the other hand, users who have a negative privacy preference will achieve more service utility by using the multilevel privacy control method (H8).

2.4 | Research model

Figure 2 depicts the research model that we define to analyze the effect of privacy-related factors on users' utility-privacy trade-offs made by using the multilevel privacy control method. For this, the hypotheses (H1 to H8) that we posed in Section 2.3 are related to the privacy control methods and the users' utility-privacy trade-offs.

By proving the first and second hypotheses (H1 and H2), we can show that different privacy control methods make users perform different utility-privacy trade-offs. If the third and fourth hypotheses (H3 and H4) are proven, we can say that the trustworthiness of a mobile application can be mitigated using the multilevel privacy control method. The fifth and sixth hypotheses (H5 and H6) are used to show how the quality level of private information affects the utility-privacy trade-offs when using different privacy control methods. The effects of users' different tendencies toward information privacy can be analyzed using the seventh and eighth hypotheses (H7 and H8).

3 | USER SURVEY

3.1 | Design of the user survey

A scenario-based questionnaire [20] was selected for overcoming the disadvantages of the two hypothesis testing methods employed by existing studies. The first hypothesis testing method [9,21] involves merely asking questions of participants for each hypothesis. One of the advantages of this method is the possibility of conducting large-scale surveys. However, if the participants cannot understand the exact intention of a question, they may not correctly state their privacy preferences. Furthermore, it may not be possible to validate a hypothesis if the questionnaire does not reflect the practical usage patterns of users. The second hypothesis testing method [17,18,20,22] comprises a demonstration application or a simulation tool that allows participants to experience a set of proposed features, and

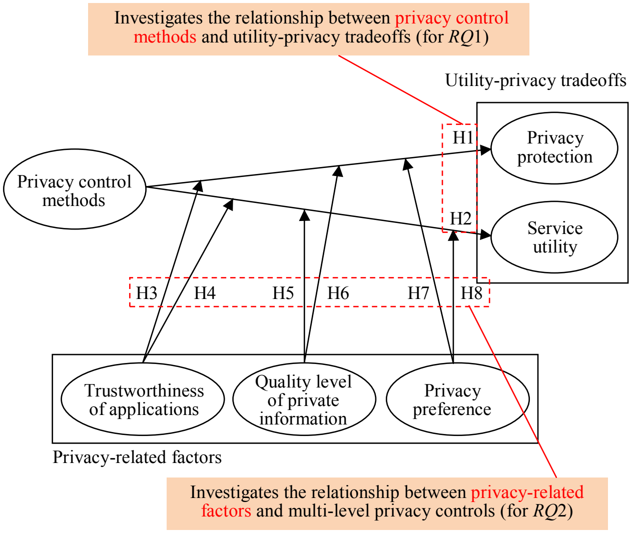

Investigates the relationship between privacy control methods and utility-privacy tradeoffs (for RQ1)
Utility-privacy tradeoffs
H1
Privacy protection
Privacy control methods
H2
Service utility
H3
H4
H5
H6
H7
H8
Trustworthiness of applications
Quality level of private information
Privacy preference
Privacy-related factors
Investigates the relationship between privacy-related factors and multi-level privacy controls (for RQ2)

FIGURE 2 Research model to analyze the effects on utility-privacy trade-offs

then validates a hypothesis based on the privacy control patterns generated by the participants. This approach thereby helps in identifying the applicable privacy control patterns of the participants. However, because the participants may not be familiar with the demonstration application or the simulation tool, this approach facilitates the collection of different data from those of the participants' usual privacy control patterns.

The user survey has been designed to reflect practical mobile computing scenarios. The authors have focused on studying users in mobile computing environments, because they have become the most popular and common computing environments employed by people worldwide. Furthermore, applications that run in mobile computing environments generally incorporate regular private information [8]. We defined a set of realistic scenarios of accessing services from mobile applications under different situations and circumstances involving disclosure of users' private information. Different from the existing studies that simply asked users' privacy preferences on mobile applications, our user survey was conducted in a way that users can actually consider the practical situations of performing their privacy controls on mobile applications. In addition, our user survey was conducted to answer our research questions by testing the hypotheses on the basis of the research model described in Section 2.4.

Regarding the privacy control method, we asked the participants to consider both the binary and the multilevel privacy control methods for the same situation in the user survey. When the binary privacy control method was presented, users could only answer either "allow" or "deny" when disclosing their private information in a given situation. Using the multilevel privacy control method, users could select one of the five QoPI levels, as described in Section 2.2.

Regarding the trustworthiness of the mobile application, in order to observe the difference in a user's privacy decisions according to the trustworthiness of the mobile application, we let the users choose the most trustworthy and untrustworthy applications among 10 candidate mobile applications. In particular, these candidate applications were chosen among the top three applications from the 10 most popular categories in the domestic Android market during the survey period. In order to perform cross-validation, the participants were asked to provide the reasons for considering a specific application as the most trustworthy or untrustworthy among multiple candidate applications.

The quality level of private information was determined on the basis of its confidentiality. According to Halsum et al., the confidentiality of information represents the confidence factor of the level of the information [23]. Although the type of private information is fixed, the value of private information can affect the confidentiality of private information. For example, for locational information, low-precision locational information such as the name of a city where a user resides is regarded as low-quality private information. However, the user's home address is regarded as high-quality private information.

In the user survey, users' privacy preferences are determined from their privacy decisions made by using the binary privacy control method rather than by asking them to describe their own privacy preferences. This is because there is a concern about the privacy paradox phenomenon, which indicates a difference between the users' privacy concerns and their actual privacy behaviors [3]. We assumed that a user has a positive privacy preference if he/she provided high-quality private information to the most untrustworthy mobile application. Users with negative privacy preferences were identified by checking whether they did not provide even low-quality private information to the most trustworthy mobile application. We classified other types of users as having neutral privacy preferences.

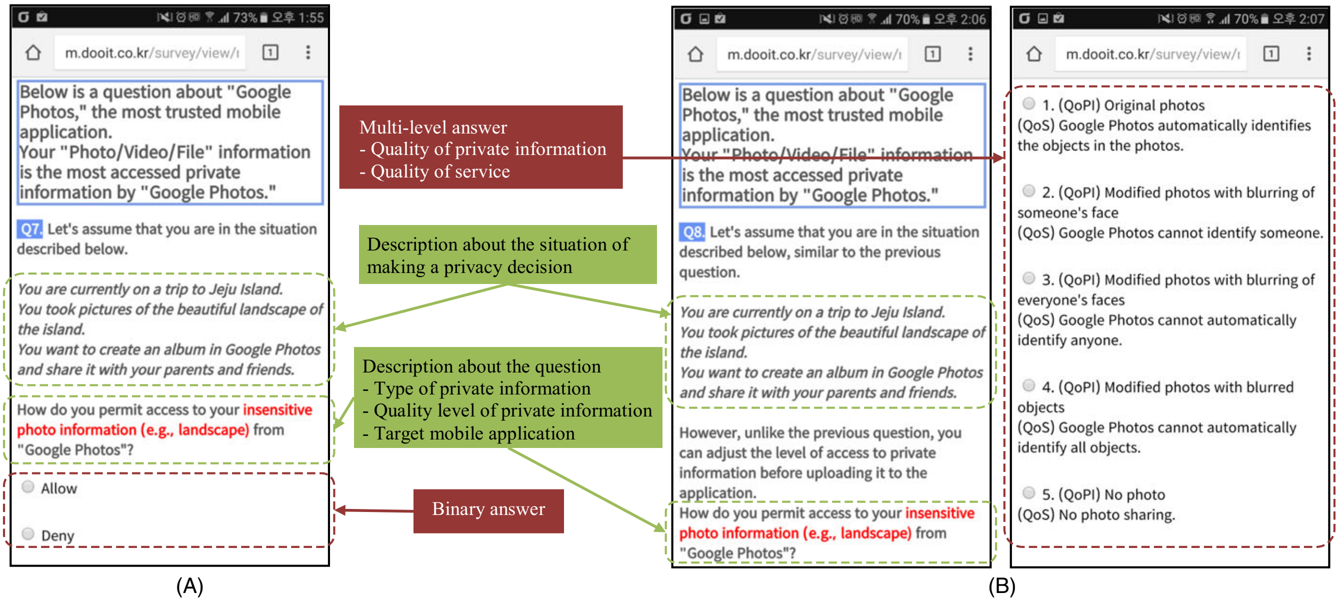
3.2 | Survey scenarios

We created eight different scenarios of disclosing users' private information for accessing services from mobile applications. The scenarios were devised by considering the different perceived trustworthiness of mobile applications (trustworthy vs untrustworthy), different perceived levels of private information (high vs low), and privacy control methods that were available (binary vs multilevel). Table 1 lists how each scenario reflects a situation in which the different values of the privacy-related factors are represented.

The questionnaires were prepared by considering each participant's privacy-related preferences, such that they could easily imagine the real situations of using the mobile applications. For each questionnaire, a sample value of private information was provided to the participants so that they could easily gauge the level of the private information

TABLE 1 Characteristics of beta-ray-emitting radioisotopes

No.	Trustworthiness of an application	Quality level of private information	Privacy control method
Q1	Trustworthy	Low	Binary
Q2			Multilevel
Q3		High	Binary
Q4			Multilevel
Q5	Untrustworthy	Low	Binary
Q6			Multilevel
Q7		High	Binary
Q8			Multilevel



Below is a question about "Google Photos," the most trusted mobile application.
Your "Photo/Video/File" information is the most accessed private information by "Google Photos."

Q7. Let's assume that you are in the situation described below.

You are currently on a trip to Jeju Island. You took pictures of the beautiful landscape of the island. You want to create an album in Google Photos and share it with your parents and friends.

How do you permit access to your insensitive photo information (e.g., landscape) from "Google Photos"?

○ Allow

○ Deny

Below is a question about "Google Photos," the most trusted mobile application.
Your "Photo/Video/File" information is the most accessed private information by "Google Photos."

Q8. Let's assume that you are in the situation described below, similar to the previous question.

You are currently on a trip to Jeju Island. You took pictures of the beautiful landscape of the island. You want to create an album in Google Photos and share it with your parents and friends.

However, unlike the previous question, you can adjust the level of access to private information before uploading it to the application.
How do you permit access to your insensitive photo information (e.g., landscape) from "Google Photos"?

○ 1. (QoPI) Original photos
(QoS) Google Photos automatically identifies the objects in the photos.

○ 2. (QoPI) Modified photos with blurring of someone's face
(QoS) Google Photos cannot identify someone.

○ 3. (QoPI) Modified photos with blurring of everyone's faces
(QoS) Google Photos cannot automatically identify anyone.

○ 4. (QoPI) Modified photos with blurred objects
(QoS) Google Photos cannot automatically identify all objects.

○ 5. (QoPI) No photo
(QoS) No photo sharing.

Multi-level answer
- Quality of private information
- Quality of service

Description about the situation of making a privacy decision

Description about the question
- Type of private information
- Quality level of private information
- Target mobile application

Binary answer

FIGURE 3 Sample questionnaires used for the user survey: (A) sample questionnaire for the binary privacy control method and (B) sample questionnaire for the multilevel privacy control method

to be sent to a mobile application. The way of answering the questionnaires and the provision of QoS information are the only differences between the questionnaires for the binary privacy control method and those for the multilevel privacy control method. In addition, the five-level QoS that was mapped to the quality levels of private information was provided to the participants.

Figure 3 shows screenshots of the questionnaires presented to the participants during the user survey. Figure 3A shows questionnaire for the binary privacy control, and Figure 3B shows that for the multilevel privacy control. As shown in the figure, these two cases present the same description of a practical situation of using a mobile application, the name of the target mobile application (ie, Google Photos), the type of private information requested by the mobile application (ie, photo and video), and the level of the private information (ie, low). As mentioned earlier, the only difference between these two cases is the way of answering the questionnaire (binary vs multilevel) and providing QoS information of the application.

3.3 | Participants

The participants were recruited from among a panel in an online survey agency.[1] Therefore, we were able to investigate privacy decisions made by typical mobile users with various demographics in terms of their gender, age, and occupation. The content and method of the user survey were approved by our Institutional Review Board (IRB) committee. Out of the total number of respondents that were asked, 548 respondents (50%) participated in the user survey. Among them, 516 participants finished the survey and received a compensation of 1,700 KRW (1.5 USD). The proposed user survey was conducted with a confidence level of 95% and an error margin of ±4.32% [24]. The demographics of the participants are listed in Table 2. The sex ratio was 4:6 in favor of females. The ages and occupations of the participants were diverse.

TABLE 2 Demographics of the survey participants

Variable	Category	Number (%)
Gender	Male	188 (36)
	Female	328 (64)
Age	20–29	148 (29)
	30–39	237 (46)
	40–49	121 (23)
	50+	10 (2)
Occupations	Other businesses	181 (35)
	Office worker	149 (29)
	Student	76 (15)
	Housewife	64 (12)
	Others (no job or else)	46 (9)

3.4 | Survey procedure

The overview of the survey procedure is as follows. First, a participant is asked to select an application that he/she thinks to be the most trustworthy among the candidate applications shown on the survey screen. The application selected by the participant is used as the trustworthy application that will be

[1] http://www.dooit.co.kr/

considered for the next four questions in the survey scenario. In addition, the participant is asked for the reason why he or she selected the application as the most trustworthy.

Second, as shown in Table 1, the participant is asked to make a privacy decision for disclosing low-quality private information to the trustworthy application by using the binary privacy control method (Q1). Next, the participant is asked to make a privacy decision by using the multilevel privacy control method under the same situation (Q2). This survey procedure is designed intentionally in this sequence because the main purpose of the survey was to observe how participants who are familiar with the binary privacy control method behave differently when they are presented with the multilevel privacy control method.

Third, in the next two questions, the participant is asked to make privacy decisions for disclosing high-quality private information to the trustworthy application by using each of the privacy control methods (Q3 and Q4). Fourth, the participant is asked to select the application that he or she thinks to be the most untrustworthy among the candidate applications and to provide the reason for selecting the application. Then, in the next four questions, the participant is asked to make privacy decisions for each type of private information for the untrustworthy application by using each of the privacy control methods (Q5–Q8). Finally, the participant is asked to give feedback on the usability of the multilevel privacy control method in a five-level Likert scale: Level 1 (very easy) to Level 5 (very difficult).

4 | ANALYSIS OF SURVEY RESULTS

4.1 | Analysis of our research model

We used the partial least squares-structural equation modeling (PLS-SEM) method to analyze our research model. In particular, we used the SmartPLS tool, which is one of the most popular tools used for PLS-SEM analyses [25]. This method measures the complex cause-effect relationships among given factors. Especially, it focuses on maximizing the explanatory power of the variables in the model rather than on the statistical accuracy of the estimate. Because we did not know whether each factor was an appropriate variable and whether there were sufficient sample data, we found formative and reflective constructs by using the PLS-SEM method. This method has also been used for similar purposes in other related studies [4,26].

To evaluate the goodness of fit of our research model, we used the R^2 score, which assesses the structural model's explanatory power. According to Cohne's study, the R^2 score classifies the effectiveness of a structural model into three levels: low ($0.02 \le R^2 < 0.13$), middle ($0.13 \le R^2 < 0.26$), and high ($R^2 \ge 0.26$) [27]. As shown in Figure 4, the R^2 score of privacy protection was 0.325 and that of service utility was 0.360. Both the R^2 scores were higher than 0.26, indicating that our research model had a moderate fit.

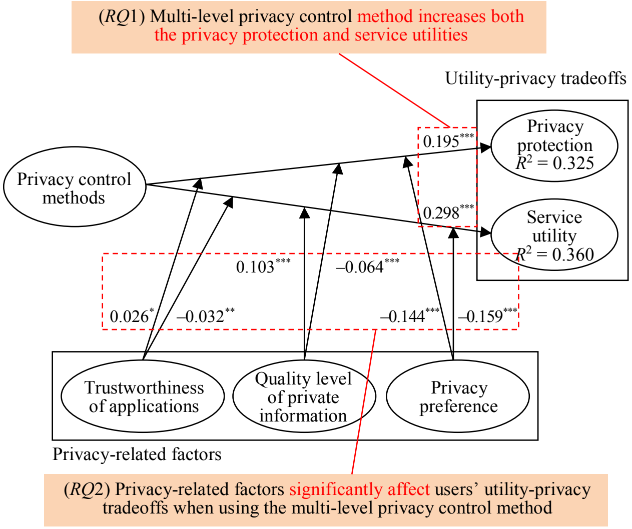

(RQ1) Multi-level privacy control method increases both the privacy protection and service utilities
Utility-privacy tradeoffs
Privacy protection $R^2 = 0.325$
Service utility $R^2 = 0.360$
Privacy control methods
0.195***
0.298***
0.103***
−0.064***
0.026*
−0.032**
−0.144***
−0.159***
Trustworthiness of applications
Quality level of private information
Privacy preference
Privacy-related factors
(RQ2) Privacy-related factors significantly affect users' utility-privacy tradeoffs when using the multi-level privacy control method

FIGURE 4 PLS-SEM analysis results of our research model

Next, we applied the bootstrapping procedure to check the validity of each item of our research model [28,29]. This enabled us to measure the significance level of the relationship between the independent variables and the dependent variables. The result of the bootstrapping with 500 samples showed that the relationship between the variables of each path in our model was statistically significant ($P < 0.05$). Except for two paths of the privacy preference with the trustworthiness of applications (service utility = 0.007, privacy protection = 0.030), the remaining six paths showed P values of <0.001.

Then, we tested the direct and indirect relationship between the factors of our research model to verify our hypothesis. Figure 4 shows the results of the PLS analysis of our research model, which summarizes our hypothesis testing. Each path shows its path coefficients (β's) and p values.

For the response to *RQ1*, our results showed that the multilevel privacy control method provided more effective utility-privacy trade-offs than the binary privacy control method. Figure 4 shows the relationship of the privacy control method with the service utility and privacy protection. The privacy control method had a positive relation with privacy protection ($\beta = 0.195$, $t = 27.359$). This means that the multilevel privacy control method increased the privacy protection compared with the binary privacy control method, supporting *H1*. Moreover, the privacy control method had a positive relation with service utility ($\beta = 0.298$, $t = 27.210$). This means that the multilevel privacy control method increased the service utility compared with that of the binary privacy control method, supporting *H2*. Therefore, the above two results answered *RQ1* affirmatively.

For the response to *RQ2*, we confirmed that privacy-related factors affected users' utility-privacy trade-offs in the multilevel privacy control method. To answer this question, we ran our research model with half of the participants' answers using the multilevel privacy control method. The goodness of fit of the model showed a medium level of effectiveness (R^2 score of service utility = 0.142, R^2 score of privacy protection = 0.162). Moreover, the result of the bootstrapping with 500 samples showed that all paths were statistically significant ($P < 0.001$; except for the path from the quality level of private information to the service utility, at $P < 0.05$). Therefore, we can conclude that all three privacy-related factors significantly affect users' utility-privacy trade-offs in multilevel privacy control method, solving *RQ2*.

4.2 | Analysis of our hypotheses

We used a *t*-test to compare the level of the difference between the binary privacy control method and the multilevel privacy control method in each hypothesis. In particular, a paired t-test was used because a participant answered the same survey question in both privacy control methods. To verify each hypothesis, referring to each type of factor in the hypothesis, we divided the results of the participants' privacy decisions by each privacy control method. Then, if the type of factor mentioned in the hypothesis showed more improvement than the other type of factor, we concluded that the hypothesis was supported.

Table 3 shows a summary of the hypothesis testing results. The increased mean rates of the multilevel method shown in the table are the improvements made by using the multilevel privacy control method compared with using the binary privacy control method. For the effectiveness of utility-privacy trade-offs according to the types of privacy control methods, the analysis result showed that the participants' privacy protection (H1) and service utility (H2) increased when using the multilevel privacy control method. For the degree of privacy protection and service utility according to the trustworthiness of applications, the privacy protection of trustworthy applications (H3) and the service utility of untrustworthy applications (H4) increased more using the multilevel privacy control method. For the degree of privacy protection and service utility according to the quality level of private information, we can conclude that the service utility of high-quality private information (H5) and the privacy protection of low-quality private information (H6) increased more using the multilevel privacy control method. Lastly, for the degree of privacy protection and service utility according to users' privacy preferences, we can conclude that the privacy protection achieved by users with optimistic privacy preferences (H7) and the service utility of pessimistic users (H8) increased more by using the multilevel privacy control method.

5 | DISCUSSIONS

Our findings suggest that the multilevel privacy control method has a positive impact on both service utility and privacy protection. In the binary privacy control method, users were forced to select either service utility or privacy protection without fully representing their utility-privacy trade-offs. However, because the multilevel privacy control method can express the users' utility-privacy trade-offs in a fine-grained manner, the users increased their service utility and privacy protection. This study has statistically proven that both participants' service utility and privacy protection increased in the same situation when using the multilevel privacy control method, compared with using the binary privacy control method. Based on these results, an investigation of whether the multilevel privacy control method actually helps users make better utility-privacy trade-offs in practical mobile computing environments is necessary.

Our findings also suggest that users showed increased consideration for the opposite side of their privacy preference in the multilevel privacy control method. Our hypotheses assumed that the multilevel privacy control method helps users to make more efficient utility-privacy trade-offs than the binary privacy control method. As the survey results show, participants consider more strongly the service utility (in the case of an untrustworthy application, high-quality level of private information, and pessimistic privacy preference) and the privacy protection (in the case of a trustworthy application, low-quality level of private information, and optimistic privacy preference), which were abandoned in the binary privacy control method. Based on these results, we can expect how users make their privacy decisions when using the multilevel privacy control method.

The results of our study may be limited by some issues with validity, as follows. First, although our user survey effectively showed the difference between each privacy-related factor when using the privacy control methods, it depended heavily on the users' response to the survey questionnaire, as in existing studies. Each user may have his/her own understanding of the situation presented in each question and make his/her privacy decision differently in practical mobile computing environments. To solve this problem, we tried to minimize the users' misunderstanding of the survey questionnaire. To measure the trustworthiness of an application, we presented the participants with 10 candidate applications and asked them to choose the most trustworthy and untrustworthy applications. In our user survey, each participant was asked to select these applications, which were then used in the context of the situation of the survey questions. In addition, to identify the users' privacy preferences, we derived three types of privacy preference from the participants' binary privacy decisions in specific

TABLE 3 Hypothesis testing results

		Privacy protection method (Mean/SD)					
ID	**Utility-privacy trade-off (privacy-related factor)**	**Binary**	**Multi-level**	***t*-value**	***p*-value**	**Increased mean rate of multilevel method**	**Results**
H1	Users' Privacy Protection (PP)	0.52/0.01	0.71/0.08	**14.37**	**<0.001**	**36.4%**	Accept
H2	Users' Service Utility (SU)	0.48/0.09	0.77/0.08	**21.22**	**<0.001**	**55.3%**	Accept
H3	PP (Trustworthy applications)	0.37/0.14	0.58/0.17	**12.20**	**<0.001**	**58.5%**	Accept
	PP (Untrustworthy applications)	0.68/0.15	0.84/0.09	10.45	<0.001	24.3%	
H4	SU (Trustworthy applications)	0.63/0.14	0.89/0.07	15.97	<0.001	41.1%	Accept
	SU (Untrustworthy applications)	0.32/0.15	0.64/0.19	**16.98**	**<0.001**	**100.0%**	
H5	SU (High quality of private information)	0.35/0.13	0.74/0.11	**22.63**	**<0.001**	**109.9%**	Accept
	SU (Low quality of private information)	0.60/0.12	0.79/0.09	12.01	<0.001	31.5%	
H6	PP (High quality of private information)	0.65/0.13	0.78/0.10	8.30	<0.001	19.7%	Accept
	PP (Low quality of private information)	0.40/0.12	0.65/0.12	**14.64**	**<0.001**	**63.5%**	
H7	PP (Optimistic privacy preferences)	0.10/0.02	0.53/0.14	**12.25**	**<0.001**	**455.3%**	Accept
	PP (Pessimistic privacy preferences)	0.88/0.04	0.87/0.04	–0.28	0.39	–0.9%	
H8	SU (Optimistic privacy preferences)	0.90/0.02	0.95/0.02	2.67	<0.001	4.4%	Accept
	SU (Pessimistic privacy preferences)	0.13/0.04	0.65/0.13	**15.40**	**<0.001**	**418.0%**	

*Bold texts mean more significant result between privacy-related factors in each hypothesis.

situations. These procedures were followed in an attempt to increase the clarity of the survey's results, and to prevent the privacy paradox phenomenon.

Second, the users may be concerned about the low level of usability owing to the hassle of choosing an appropriate level in the multilevel privacy control method. Users can experience difficulty in making fine-grained privacy decisions in the multilevel privacy control method, compared with the simple binary answer in the binary privacy control method. To check the usability issue, in the last question of our user survey, we asked participants to answer the usability of the multilevel privacy control method. According to the participants' responses, the average score was middle (M = 3.13, SD = 0.92) (Level 1: very easy; Level 5: very difficult). Therefore, we can conclude that the participants did not experience low usability when using the multilevel privacy control method. In addition, it may be possible to reduce the users' burden of executing multilevel privacy controls by learning the users' previous privacy decisions associated with privacy-related factors such as the trustworthiness of an application, quality level of private information, and users' privacy preferences, and recommending an appropriate level of privacy control to the users for a given situation.

6 | RELATED WORK

There have been some studies performed on modeling and analyzing users' privacy decisions based on the privacy calculus theory, as discussed in Section 2. They conducted user surveys to identify the core factors that affect users' privacy decisions and the relationships among them. As a result, some of the studies found a set of privacy-related factors that affect users' privacy-utility trade-offs. In addition to identifying privacy-related factors in our study, we also analyzed the effectiveness of using the QoPI model to represent multiple abstraction levels of private information, associating it with the corresponding QoS that can be obtained from mobile applications.

Berezowska et al. found that users' privacy concerns were mainly affected by the availability of information controls that prevent service providers from misusing their private information [21]. However, the types and quality of information controls vary depending on the service provider, and users are not allowed to control the amount of private information they can provide in exchange for accessing services from an application. Knijnenburg and Kobsa examined the relationship between coarse-grained and fine-grained privacy controls. They found that when the fine-grained option is not available, users often choose the coarse-grained option that is closest to the previously selected fine-grained option for an application [22]. In our study, we showed that the coarse-grained privacy controls (binary controls) supported by most mobile platforms are insufficient for users to make utility-privacy trade-offs. Therefore, we suggested a five-level privacy control method that can be selected based on the QoS required by users. Zhang et al. also showed that the availability of fine-grained privacy controls effectively eased users' concerns about providing their private information to applications [20]. However, their study focused mostly on examining users' different privacy concerns based on the availability of privacy controls. In contrast, our study focused on analyzing users' utility-privacy trade-off patterns based on different privacy control methods.

Knijnenburg and Kobsa found that users' privacy preferences and applications' justification for requesting private information were essential factors that influenced users' privacy decisions [17,18]. Usually, an application's justification for accessing a user's private information is provided in the form of a message to the user. However, these justification messages are often vague and sometimes even unavailable. Therefore, it is difficult for users to make appropriate privacy decisions purely based on the justification messages provided by applications. Ting and Till revealed that the perceived service quality of an application is more important for users than the privacy concerns related to accessing the application [4]. However, the perceived service quality of an application may vary across different users. Therefore, in our study, rather than asking the user to consider the perceived service quality of an application, we allowed the user to assess the quality of service provided by the application according to the quality of private information to which the user explicitly permits access.

7 | CONCLUSIONS AND FUTURE WORK

In this study, we investigated whether the multilevel privacy control method improved users' utility-privacy trade-offs. We assumed that users make different privacy decisions when they use different privacy control methods, and we conducted a user survey to validate this assumption. The user survey was designed to allow participants to consider eight different situations involving the use of mobile applications with different combinations of privacy-related factors. We observed how the changes in privacy control methods affected the users' service utility and privacy protection. As a result, we found that the use of the multilevel privacy control method improved the service utility and privacy protection compared with the use of the binary privacy control method. We also found that the privacy-related factors did affect the users' privacy decisions, especially when they used the multilevel privacy control method.

The main contributions of our work are as follows. First, we verified that users' utility-privacy trade-offs can be improved using the multilevel privacy control method. In other words, by using the multilevel privacy control method, users can improve both the service utility and privacy protection under practical situations involving the use of mobile applications. The service providers can also offer their services to more users and provide more personalized services that the users want to access while protecting their privacy.

Second, we identified the users' different privacy decisions when they used the multilevel privacy control method according to the privacy-related factors. Based on the analysis result, we can recommend users an appropriate quality level of private information to be provided to a mobile application by considering the privacy-related factors. This allows users not only to conveniently use the multilevel privacy control method but also to improve both the service utility and privacy protection. To the best of our knowledge, this is the first work to investigate users' utility-privacy trade-offs when they use a fine-grained privacy control method in mobile computing environments.

In our future work, based on the results of our user survey, we will develop a multilevel privacy control method that can be integrated with practical mobile platforms. We also plan to verify that both the service utility and privacy protection can be improved using the multilevel privacy control method in practical mobile computing platforms. Based on the findings in this study, we will investigate how to predict appropriate quality and quantity levels of private information to be sent to mobile applications by considering the privacy-related factors in given situations. This will also contribute to reducing the users' burden of executing multilevel privacy controls, and allow users to perform more effective and efficient privacy-utility trade-offs when using mobile applications.

ORCID

Seung-Hyun Kim http://orcid.org/0000-0001-8934-3648

REFERENCES

1. M. Hartmann, *Mobile privacy: contexts, privacy, online*, Springer, Berlin, Heidelberg, 2011, pp. 191–203.
2. T. Dinev and P. Hart, *An extended privacy calculus model for e-commerce transactions*, Inform. Syst. Res. **17** (2006), no. 1, 61–80.
3. H. Xu et al., *The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing*, Decision Supp. Syst. **51** (2011), no. 1, 42–52.
4. T. Li and T. Unger, *Willing to pay for quality personalization? Trade-off between quality and privacy*, Eur. J. Inform. Syst. **21** (2012), no. 6, 621–642.
5. S. Petronio, *Boundaries of privacy: dialectics of disclosure*, State University of New York Press, Albany, NY, 2002.
6. M. J. Keith et al., Privacy assurance and network effects in the adoption of location-based services: an iphone experiment, *Proc. Int. Conf. Inform. Syst.*, St. Louis, MO, USA, 2010, pp. 237–255.
7. T. Dinev et al., *Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts*, Eur. J. Inform. Syst. **22** (2013), no. 3, 295–316.

8. S. H. Kim et al., Effects of contextual properties on users' privacy preferences in mobile computing environments, *IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, Aug. 20–22, 2015, pp. 507–514.
9. G. R. Milne and M. E. Boza, *Trust and concern in consumers' perceptions of marketing information management practices*, J. Interact. Market. **13** (1999), no. 1, 5–24.
10. R. K. Chellappa and R. G. Sin, *Personalization versus privacy: an empirical examination of the online consumer's dilemma*, Inform. Technol. Manag. **6** (2005), no. 2–3, 181–202.
11. S. Y. Komiak and I. Benbasat, *The effects of personalization and familiarity on trust and adoption of recommendation agents*, MIS Quarterly **30** (2006), no. 4, 941–960.
12. F. Kehr et al., *Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus*, Inform. Syst. J. **25** (2015), no. 6, 607–635.
13. H. Li, R. Sarathy, and H. Xu, *The Role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors*, Decision Supp. Syst. **51** (2011), no. 3, 434–445.
14. N. K. Malhotra, S. S. Kim, and J. Agarwal, *Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model*, Inform. Syst. Res. **15** (2004), no. 4, 336–355.
15. M. Lwin, J. Wirtz, and J. D. Williams, *Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective*, J. Acad. Market. Sci. **35** (2007), no. 4, 572–585.
16. J. Omarzu, *A disclosure decision model: determining how and when individuals will self-disclose*, Pers. Soc. Psychol. Rev. **4** (2000), no. 2, 174–185.
17. B. P. Knijnenburg and A. Kobsa, *Making decisions about privacy: information disclosure in context-aware recommender systems*, ACM Trans. Interaction Intell. Syst. **3** (2013), no. 3, 20–52.
18. B. P. Knijnenburg and A. Kobsa, Helping users with information disclosure decisions: potential for adaptation, *Proc. Int. Conf. Intell. User Interf.*, Santa Monica, CA, USA, Mar. 19–22, 2013, pp. 407–416.
19. F. Kehr et al., Rethinking privacy decisions: pre-existing attitudes, pre-existing emotional states, and a situational privacy calculus, *ECIS Proc.*, Greece, 2015, pp. 1–15.
20. B. Zhang, N. Wang, and H. Jin, Privacy concerns in online recommender systems: influences of control and user data input, *Proc. Symp. Usable Privacy Secur.*, Menlo Park, CA, USA, July 9–11, 2014, pp. 159–173.
21. A. Berezowska et al., *Consumer adoption of personalised nutrition services from the perspective of a risk–benefit trade-off*, Genes Nutrition **10** (2015), no. 6, 1–16.
22. B. P. Knijnenburg, A. Kobsa, and H. Jin, Preference-based location sharing: are more privacy options really better?, *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, Paris, France, Apr. 27–May 2, 2013, pp. 2667–2676.
23. K. Haslum, A. Abraham, and S. Knapskog, Fuzzy online risk assessment for distributed intrusion prediction and prevention systems, *Int. Conf. Comput. Modeling Simulation*, Cambridge, UK, Apr. 1–3, 2008, pp. 216–223.
24. Wikipedia. *Margin of error*, available at http://en.wikipedia.org/wiki/Margin_of_error (Apr. 18, 2018).
25. C. M. Ringle, S. Wende, and J. M. Becker, *SmartPLS 3*. Boenningstedt: SmartPLS GmbH, 2015, available at http://www.smartpls.com (Oct. 30, 2017).
26. M. J. Keith et al., *Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior*, Int. J. Human-Comput. Studies **71** (2013), no. 12, 1163–1173.
27. J. Cohen, *Statistical power analysis for the behavioral sciences*, Lawrence Erlbaum, Hillsdale, NJ, 1988.
28. M. Tenenhaus et al., *PLS path modeling*, Comput. Stat. Data Anal. **48** (2005), no. 1, 159–205.
29. D. Temme, H. Kreis, and L. Hildebrandt, *PLS path modeling—a software review*, SFB 649 Discussion Paper 2006-084, Institute of Marketing, Berlin, Germany, 2006.

AUTHOR BIOGRAPHIES

Seung-Hyun Kim has been a member of the research staff of the Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea, since 2004. He received his PhD in computer science in 2017 from the Korea Advanced Institute of Science and Technology, Daejeon, Rep. of Korea. His main research areas are ID management, web security, mobile privacy, and block-chain privacy.

In-Young Ko is an associate professor in the school of computing of the Korea Advanced Institute of Science and Technology, Daejeon, Rep. of Korea. He received his PhD in computer science in 2003 from the University of Southern California, Los Angeles, CA, USA. His research interests include software engineering, web engineering, and service computing.