View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by ScholarWorks@UNIST

creative commons

C O M M O N S D E E D

저작자표시-비영리-변경금지 **2.0** 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

Master's Thesis

The Impacts of Privacy Rules on Users' Perception on Internet of Things (IoT) Applications:

Focusing on Smart Home Security Service

Mingyung Kim

Department of Management Engineering

Graduate School of UNIST

2017

The Impacts of Privacy Rules on Users' Perception on Internet of Things (IoT) Applications: Focusing on Smart Home Security Service

Mingyung Kim

Department of Management Engineering

Graduate School of UNIST

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

The Impacts of Privacy Rules on Users' Perception on Internet of Things (IoT) Applications: Focusing on Smart Home Security Service

A thesis/dissertation
submitted to the Graduate School of UNIST
in partial fulfillment of the
requirements for the degree of
Master of Management Engineering

Mingyung Kim

07. 07. 2017 Month/Day/Year of submission

Approved by

Advisor
Boreum Choi

The Impacts of Privacy Rules on Users' Perception on Internet of Things (IoT) Applications: Focusing on Smart Home Security Service

Mingyung Kim

This certifies that the thesis/dissertation of Mingyung Kim is approved.

07. 07. 2017

Signature

Advisor: Boreum Choi

Signature

Yoonhyuk Jung

Signature

Molan Kim

The Impacts of Privacy Rules on Users' Perception on Internet of Things (IoT) Applications: Focusing on Smart Home Security Service

Abstract

As communication and information technologies advance, the Internet of Things (IoT) has changed the way people live. In particular, as smart home security services have been widely commercialized, it is necessary to examine consumer perception. However, there is little research that explains the general perception of IoT and smart home services. This article will utilize communication privacy management theory and privacy calculus theory to investigate how options to protect privacy affect how users perceive benefits and costs and how those perceptions affect individuals' intentions to use of smart home service. Scenario-based experiments were conducted, and perceived benefits and costs were treated as formative second-order constructs. The results of PLS analysis in the study showed that smart home options to protect privacy decreased perceived benefits and increased perceived costs. In addition, the perceived benefits and perceived costs significantly affected the intention to use smart home security services. This research contributes to the field of IoT and smart home research and gives practitioners notable guidelines.

Keywords: Internet of Things, Smart home, Privacy rule, Security

Contents

I. Introduction……1

II. Literature Review……4

- 2.1. Smart Home……4
- 2.2. Privacy Controls……4
- 2.3. Privacy Calculus……5

III. Hypotheses……7

IV. Methods……10

- 4.1. Participants……10
- 4.2. Measurements……11
- 4.3. Stimuli……11

V. Results……12

- 5.1. Measurement Model……12
- 5.2. Hypothesis Testing……13
- 5.3. Supplementary Analysis……14

VI. Discussion……16

VII. Implications, Limitations, Future Research, and Conclusions……17

- 7.1. Theoretical Implication……17
- 7.2. Practical Implication……17
- 7.3. Limitations and Future Research……18
- 7.4. Conclusion……19

List of Tables

Table1. Measurement Items……………………………………………………10

Table 2. Reliability and Convergent Validity……………………………….………12

Table 3. Discriminant Validity…………………………………………………13

List of Figures

Figure 1. Market Size of Smart Home……………………………………………...…1

Figure 2. Survey of Barriers to Investing in the IoT…………………………..…2

Figure 3. Research Model…………………………………………………………9

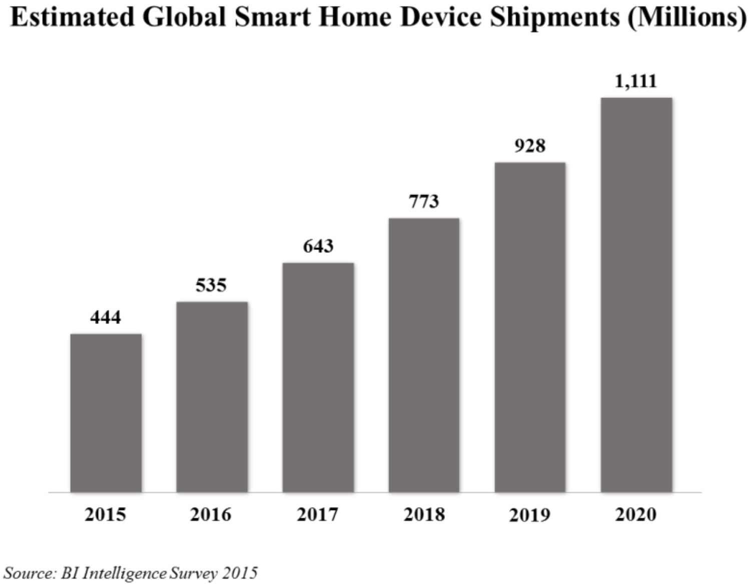
Figure 4. Results of Research Model……………………………………………..14

Figure 5. Effects of Smart Home Service Options on Perceived Benefits…….15

Figure 6. Effects of Smart Home Service Options on Perceived Risks………..15

I. Introduction

As communication and information technologies have advanced, the Internet of Things (IoT) has changed the way people live. Machines can collect data, transmit information, and process the information independently (Louis, 2011). The number of connected devices, such as wearables, appliances and automobiles, will exceed 18 billion worldwide by 2018 (Kiat, Mojy, Tony and Do, 2014). The IoT has a lot of applications in various fields, such as health monitoring, smart cars, and smart homes. In particular, it is expected that the number of smart home devices shipped will grow to 1,111 million in 2020, including all smart appliances and smart home safety and security systems (Figure 1).



Source: BI Intelligence Survey 2015

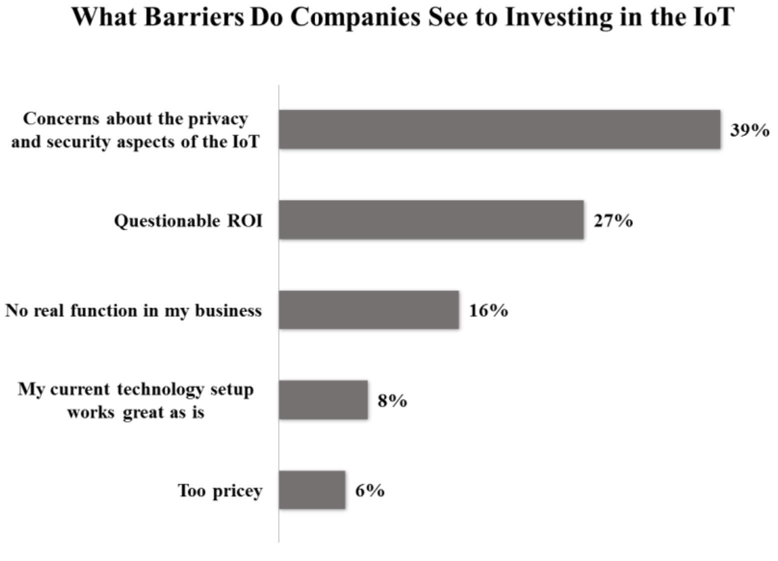
Figure 1. Market Size of Smart Home

What people most likely expect when using IoT devices is constant monitoring and linked, real-time data transmission with personalized recommendations and immediate responses (Swan, 2012). IoT's enhanced connectivity has resulted in a technology that can by used for anything, at any time, at any place, and by anyone. (Louis, 2011). The IoT encourages the communication between devices and allows users to automate and control tasks in their daily lives. For example, users can control their home's lighting via their smartphone without actually being home.

With the big opportunities of the IoT, concerns about security and privacy have been raised. For example, in the case of smart home, when uses disclose personal information to receive smart home services,

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

unknown third parties may also be able to analyze their daily patterns. For example, third parties may be able to determine things such as when and where the user ate. Gartner (2016) identified IoT security as one of the most important aspects of IoT technologies. BI Intelligence, a research company, conducted a survey showing that the biggest obstacle for investing in the IoT is concerns about the privacy and security aspects (Figure 2). There is the possibility that user information can be leaked by unauthorized third parties and be abused. Therefore, it is necessary to conduct research on IoT privacy and security issues.



Source: BI Intelligence Survey 2015

Figure 2. Survey of Barriers to Investing in the IoT

In some case, disclosure of personal information is a prerequisite to access additional services and is requested for these services to be personalized (Shih, Hsu, Yen, and Lin, 2012). When people share their personal information, however, they estimate the cost as well as the benefits (Acquisti and Grossklags, 2005). Studies have been conducted on privacy issues surrounding Social Network Services (SNS) and many studies concluded that privacy concerns have a significant effect on choosing whether to share personal information (Wu, Huang, Yen, Popova, and Zlatolas, 2012; Zlatolas, Welzer, Hericko, and Holbl, 2014).

Most previous studies regarding the IoT focused on technological aspects (Thin et al., 2015). Although a few studies explain the importance of privacy issue (Farooq, Waseem, Khairi, & Mazhar, 2015; Gubbi, Buyya, Marusic, & Palaniswami, 2013; Swan, 2012), there is still a lack of research that empirically explains the relationship between privacy and the IoT. In particular, most previous research on smart homes was qualitative research focused on assisted living applications for elderly or disabled occupants (Demiris & Hensel, 2008; Ding & Gebel, 2012; Eriksson & Timpka, 2002). It is necessary to conduct empirical research from the perspective of regular individuals.

The purpose of this study is to investigate what kind of smart home service options maximize perceived benefits and minimize perceived costs and how perceived benefits and risks affect users' intention to use smart home services. The theories of communication privacy management and privacy calculus are important and notable theories in the field of management information systems. Especially, the communication privacy management theory highlights the importance of an individual's ability to deal with privacy risks and helps explain the motivations for self-disclosure. In the context of smart homes, analyzing whether people reveal their private information is an important issue. Therefore, using communication privacy management theory is reasonable. The privacy calculus theory is the most common approach to analyzing personal information disclosure behavior. By emphasizing trade-off interrelation of self-disclosure, privacy calculus can be used to determine individuals' intentions to use smart home services.

II. Literature Review

2.1 Smart Home

The IoT concept can be utilized in a wide range of fields, such as smart environments, transportation, and healthcare (Seo, Kim, Kim & Lee, 2016). Specifically, in 2015, the number of devices connected with smart homes was approximately 294,200,000 (Gartner, 2015; Seo et al., 2016). In particular, "smart home" means automated services that can control and manage devices in the home locally or remotely (Jeong, Salvendy, & Proctor, 2010). Briere (2011) defined a smart home as "a harmonious home, a conglomeration of devices and capabilities working through home networking" (Jeong et al., 2010). Integration of home-based networks into smart homes is expected to develop some beneficial properties.

Smart home services can be divided into three categories: Security, energy management, and lifestyle support (Balta-Ozkan, Davidson, Bicket, & Whitmarsh, 2013). Smart home security services offer the ability to monitor movement in and near the home, identify potential intruders, alert users about open doors and windows, and deter thieves from a temporarily unoccupied property. Smart home energy management services assist in reducing energy demands by reducing the heating on hot sunny days and by supplying data about real-time energy usage and energy bill. Finally, smart homes support services such as monitoring user activity and analyzing and providing alerts for potential accidents or dangers. Among the three services, this paper focused on security. According previous surveys, many people felt that smart home safety and security services are a top priority for their own houses (Bierhoff et al., 2007). In addition, security service at home is one of the most commercialized smart home services. Specifically, 62% of users use smart home services to remotely manage their home alarms and one in five people interact with their smart home systems mainly for security and safety (Gartner, 2015). Therefore, conducting an experiment based on smart home security services makes sense.

2.2 Privacy Controls

Communication privacy management (CPM) theory reveals a process in which users decide between sharing information with others and privacy concerns (Metzger, 2007). When people disclose their information, they form informational boundaries that encompass information they do not want to reveal, and the information that can be shared is determined through such boundaries (Y. Li, 2012; Petronio, 2010). This theory allocates a level of perception to how people establish, manipulate, and exchange their private information. Petronio (2001) stated five core principals that determine how people disclose personal information. People manage their personal information in accordance with their personal privacy rules with the belief that they have the right to own and control their personal information (Petronio, 2001). When people share or give others access to their personal information, they become co-owners of that information (Petronio, 2001). Then, people need to gradually negotiate privacy rules with the co-owners of their information for controlling information, and the co-owners need to follow the privacy rule (Petronio, 2001). If the co-owners of personal information do not adhere to privacy rules, boundary turbulence may occur (Petronio, 2001).

According to the CPM theory (Petronio, 2001), people tend to make privacy rules to control their private information. Petronio (2010) suggested three privacy rules people use to make decisions about whether they disclose their personal information. The first rule is a linkage rule that people use to create a collective boundary (Lee, Park & Kim, 2013; Petronio, 2010). In the process of disclosing personal information, people can share their information boundaries and determine which additional owner can know the personal information. The second rule is a permeability rule, which regulates access to and protects personal information. In the process of permeability rule, the degree of information flow and amount of protection are determined (Lee et al., 2013). The third rule is an ownership rule defined as "an agreement about how much control others have to independently manage the private information. In some cases, co-owners have no rights of distribution and modification" (Petronio, 2010).

The rules are highly situational and may be changed to fit new or evolving circumstances (Metzger, 2007). Petronio (2010) insisted that continuous research into the various ways people apply existing privacy rules and how they respond to those rules is necessary to understand how people are changing privacy boundaries in diverse contexts. As technologies develop, information boundaries of people have been changed by ubiquitous access to information (Ji & Lieber, 2010; Li, 2012). Now, it is necessary to consider the boundaries more broadly beyond personal information revealing and concealing. This paper proposes three smart home service options based on the three privacy rules of the CPM theory.

2.3 Privacy Calculus

Privacy calculus is "a cost-benefit trade-off analysis that accounts for inhibitors and drivers that simultaneously influence the decision on whether to disclose information or not" (Dinev & Hart, 2006). When people disclose their personal information, they tend to weigh both the costs and benefits simultaneously. In some case, self-disclosure is a prerequisite to access additional services and is requested for these services to be personalized (Shih, Hsu, Yen, & Lin, 2012). When people reveal their personal information, however, they estimate the risks as well as the benefits (Acquisti & Grossklags, 2005).

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

In the privacy calculus literature, intentions to disclose information are regarded as a result of a rational, independent assessment of perceived costs and perceived benefits (Culnan & Armstrong, 1999). To date, privacy calculus theory has been generally used in various studies (Li, Sarathy, & Xu, 2011), location-based services (Xu, Luo, Carroll, & Rosson, 2011; Xu, Teo, Tan, & Agarwal, 2009; Zhao, Lu, & Gupta, 2012), and social commerce (Sharma & Crossler, 2014), etc. However, in a smart home context, there is little research that has adopted the privacy calculus theory to investigate disclosing personal information behaviors. Therefore, in this paper, the privacy calculus theory has been used for the experiments conducted.

The perceived benefits and perceived costs are especially treated as formative, second-order constructs because the increase in one dimension is not necessarily enough to instigate an increase in other factors, so formative factors are preferred over reflective representations (Luo, Li, Zhang & Shim, 2010). *Perceived benefit* is defined as “the degree to which a person believes that using the services would enhance his or her job/work/life performance” (Bauer, 1967). Personalization, and connectivity are considered as antecedent factors of perceived benefits that people most expect when using IoT services. *Personalization* is defined as “the ability to provide content and services that are tailored to individuals based on knowledge about their preferences and behaviors” (Adomavicius, & Tuzhilin, 2005). People tend to share their private information to receive personalized services (Xu et al., 2009). *Ubiquitous connectivity* is defined as “the extent to which an individual perceives that he or she is linked with products or services anytime and anywhere via smart devices” (Choi, 2016; Lee, Park & Chung, 2012; Tojib & Tsarenko, 2012). Ubiquitous connectivity is expected as a fundamental factor of satisfaction of IoT services.

Perceived cost is defined as “the perception of the user about the expense and possible loss that may be incurred when using smart device” (Pi, Liao, Liu, & Hsieh, 2010). Perceived costs has commonly identified with multidimensional nature of the perceived costs construct (Featherman & Pavlow, 2003; Luo, Li & Shim, 2010). Recent studies have been empirically conducted on the effects of the seven facets of perceived costs, including performance, financial, time, psychological, social, privacy, and overall risk (Featherman & Pavlow, 2003). Among them, this study chose privacy and time risks as factors that form perceived costs. *Privacy risk* is defined as “potential loss of control over personal information, such as when information about you is used without your knowledge or permission” (Featherman & Pavlow, 2003). *Time risk* is defined as “the time consumers may lose by wasting time researching and learning how to use a product or service only to have to replace it if it does not perform to expectations” (Featherman & Pavlow, 2003).

III. Hypotheses

Linkage smart home service options involve additionally sharing personal information with neighborhoods. By sharing personal information with other people, people may feel social risks (Acquisti & Grossklags, 2005). From the perspective of social risk, the presence of third parties increases anxiety so that perceived benefits decrease and perceived costs increase (Sherry, McGrath, & Levy, 1993; Shmargad & Watts, 2016; Wooten, 2000). According to previous research regarding social networks, people tend to perceive more risks when they share their personal information socially (Balaji, Khong, & Chong, 2016). In other words, the more people know their individual information, the higher the risk is. Similarly, in the context of smart homes, when personal information is shared with neighborhoods, the neighborhoods may be able to know when the users have come in and out of their house so that they may feel more anxiety. Thus, we can expect that a linkage option may decrease perceived benefits and increase perceived costs.

H1: Compared with no option, a linkage option will decrease perceived benefits.

H2: Compared with no option, a linkage option will increase perceived costs.

A permeability option eliminates sensitive information in advance and shares ambiguous information rather than precise information (Lee et al., 2013). By sharing private information, perceived benefits decrease. According to previous research, perceived benefits are affected by information sensitivity (Omarzu, 2000). When people disclose sensitive information, they anticipate a similar level of benefit. However, because a permeability option obscures sensitive information in advance, the sensitivity of information is reduced, so that people may anticipate a lower degree of perceived benefits. Similarly, when using smart home security service, users may perceive less benefits as they conceal their problematic information.

When using a permeability option for smart home services, users can reduce concerns about privacy risk by concealing sensitive information, but it is necessary to determine the amount and type of information that they will disclose. Previous research argued that additional time and effort increase perceived costs, because consumers tend to believe that it is a waste of time and effort (Nepomuceno, Laroche, & Richard, 2014). When using smart home security service, they have to determine what information to disclose and what information to conceal. This process require additional time and effort to use the smart homer services. Also when a friend visit their house but the friend is not registered to the smart home system, the users have to unlock the doors and windows after checking the smart home system. Therefore, we can expect that a permeability option will reduce perceived benefits and induce perceived costs.

H3: Compared with no option, a permeability option will decrease perceived benefits.

H4: Compared with no option, a permeability option will increase perceived costs.

An ownership option is used to control the rights of co-owners of personal information who receive users' individual information to provide smart home services (Petronio, 2001). In the case of no smart home service options, people do not know how provided information is used and shared. However, when ownership option is used, service providers cannot share and control users' private information and it leads the decrease of perceived benefit because the breadth of service is decreased. If smart home security service providers can share users' information, they can not only lock the doors and windows, but also report it to the police when an intruders is in the house. However, the rights of the service provider to share the users' information, they will not be able to provide additional services beyond the services provided by the smart home security service provider.

However, when control users are informed of their rights in advance, people may feel less anxiety. Thus, privacy risks may decrease. Conversely, perceived costs will increase because users need to monitor their service providers while using the smart home services to use an ownership option. Previous research suggested that time risk is one of the most important factor (Verma, Tiwari & Mishra, 2011). In particular, for ownership option, users constantly care for service providers to monitor misuse of their personal information. As a result, using an ownership option is considered as a waste of time, so that people may perceive reduced costs. Therefore, we can expect that an ownership option will increase perceived benefits and decrease perceived costs.

H5: Compared with no option, an ownership option will decrease perceived benefits.

H6: Compared with no option, an ownership option will increase perceived costs.

Privacy calculus theory emphasizes that when providers access private information, people tend to analyze the costs and benefits simultaneously that enable information disclosure (Awad & Krishnan, 2006). Many studies about self-disclosure showed that perceived benefits induced behavior intention. If people believe that they can obtain benefits by disclosing their private information, then they are willing to give up a measure of their privacy for potential benefits (Wang, Duong & Chen, 2016, Xu et al., 2011). Previous studies showed that the higher the uncertainty, the higher the perceived costs. People

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

have concerns that service providers may use their personal information without prior notice or consent (Xu et al., 2011). This uncertainty will make people reluctant to uses a smart home service.

H7: Perceived benefits positively affect intentions to use of smart home services.

H8: Perceived costs negatively affect intentions to use of smart home services.

Figure 3 shows the overall research model.

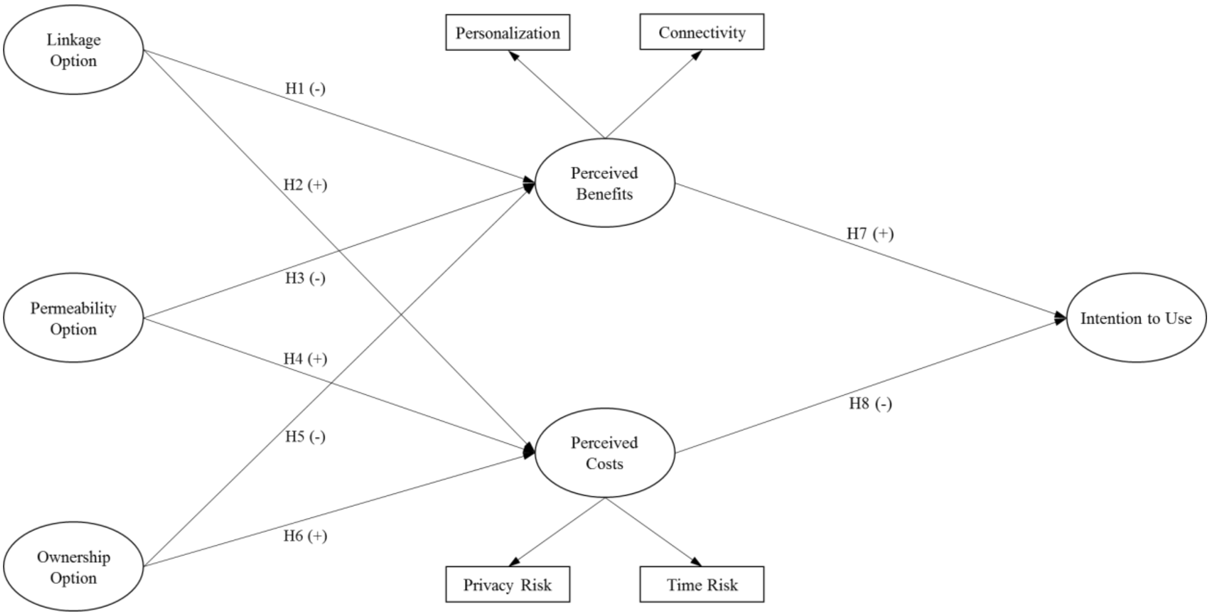

Linkage Option
Permeability Option
Ownership Option
Personalization
Connectivity
Perceived Benefits
Perceived Costs
Privacy Risk
Time Risk
Intention to Use
H1 (-)
H2 (+)
H3 (-)
H4 (+)
H5 (-)
H6 (+)
H7 (+)
H8 (-)

Figure 3. Research Model

IV. Methods

4.1 Participants

Embrain, the biggest online research agency with the largest consumer panel in Asia, was used to recruit participants. There were 399 respondents. After eliminating outliers, 335 responses were used in the analysis, with 181 males and 154 females. The age range was from 20 to 68 and the mean age was about 39.

Table1. Measurement Items

Construct	**Items**		**Reference**
Personalization	**PER1**	This smart home service understands my specific needs.	Xu et al. (2011)
	PER2	This smart home service offers me personalized services.	
	PER3	This smart home service offers recommendations that match my needs and to the situation.	
Connectivity	**CON1**	I can access to this smart home service anywhere for the necessary service.	Chun et al. (2012)
	CON2	This smart home service allows me to use home security service anywhere at anytime.	
	CON3	I can access to this smart home service any time for the necessary service.	
Privacy risk	**PR1**	Using this smart home service allows unwanted people to use my information.	Featherman and Pavlou (2003)
	PR2	If I use this smart home service, other people may use it in an inappropriate way.	
	PR3	If I use this smart home service, other people may use it in an unwanted way.	
Time Risk	**TR1**	Investing my time to use this smart home service is risky.	Featherman and Pavlou (2003)
	TR2	The possible time loss from having to set up and learn how to use this smart home service makes it.	
	TR3	If I started this smart home service, I may lose time due to switching costs.	
	TR4	I would have to waste a lot of time fixing system errors to use this smart home service.	
Intention to Use	**IU1**	I will recommend using this smart home service to others.	Chun et al. (2012)
	IU2	I intend to use this smart home service.	
	IU3	I plan to use this smart home service in the future.	

PE: Personalization, **CON:** Connectivity, **PR:** Privacy risk, **TR:** Time risk, **IU:** Intention to use

4.2 Measurements

To examine the intention to use smart home services, a scenario-based survey was conducted focusing on security services. To ensure content validity, items used to measure the constructs were modified from previous studies. All of the survey items were measured on a seven-point Likert scale, with from 7 indicating “strongly agree” to 1 indicating “strongly disagree.” The measurement items are stated in Table 1 with the references.

4.3 Stimuli

Using the CPM theory, three smart home service options are manipulated (Appendix) and it is assumed that smart home service options cannot be mixed. The situation was that sensors on doors and windows monitor movement in and near the home and collect information in real time. The collected information is automatically transmitted to security service providers. No option was if external intrusion is detected, the security services provider automatically locked doors and windows and user could check through a smartphone application.

The linkage option was for sharing information with a neighborhood. The manipulation was that if a thief breaks into a neighboring house, to prevent other accidents, the security services provider automatically locked doors and windows and users could check through a smartphone application.

The permeability option was for concealing precise information. The manipulation was that if an unregistered person entered, the security services provider automatically locked doors and windows and user could check through a smartphone application. The provided information to the service provider only about whether the person is registered rather than precise information, such as a picture.

The ownership option was for restricting the rights to control of personal information. The manipulation of the ownership option was given so that if external intrusion is detected, the security services provider automatically locked doors and windows and can check through smartphone application. The security service provider cannot reuse or modify information after providing services to the user.

V. Results

To analyze the research model in this study, the partial least square (PLS) approach was used. We analyzed the data with SmartPLS3.0. The PLS approach is usually used to validate casual relationships between constructs with multiple measurement items. Furthermore, The PLS model fits not only large sample sizes but also small sample sizes, and it readily covers formative, as well as reflective, constructs (Hair, Ringle, & Sarstedt, 2011).

5.1 Measurement Model

Reliability was measured with Cronbach's alpha and composite reliability, which both must exceed 0.70. Table 2 indicated that both composite reliabilities and Cronbach's alphas exceeded the required minimum of 0.70. Convergent validity measured via standardized factor loading must be greater than 0.70 with a t-value greater than 1.96 and the average variance extracted (AVE) must not be less than 0.50. As shown in Table 2, all standardized factor loadings are more than the required minimum of 0.70 and all AVE values exceeded the required minimum of 0.50.

Table 2. Reliability and Convergent Validity

Construct	Item	Factor	T-Value	Composite Reliability	AVE	Cronbach's α
Personalization	**PE1**	0.869	62.953	0.929	0.813	0.885
	PE2	0.815	61.780			
	PE3	0.746	55.298			
Connectivity	**CON1**	0.833	97.261	0.941	0.842	0.906
	CON2	0.814	66.517			
	CON3	0.758	72.326			
Privacy risk	**PR1**	0.928	162.189	0.965	0.901	0.945
	PR2	0.926	153.647			
	PR3	0.895	32.191			
Time Risk	**TR1**	0.863	119.596	0.931	0.771	0.904
	TR2	0.846	75.658			
	TR3	0.837	32.191			
	TR4	0.790	23.570			
Intention to Use	**IU1**	0.850	112.532	0.947	0.856	0.906
	IU2	0.842	52.154			
	IU3	0.832	81.069			

PE: Personalization, **CON:** Connectivity, **PR:** Privacy risk, **TR:** Time risk, **IU:** Intention to use

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

Discriminant validity was determined with the standard that the square root of the AVE for each construct should be not less than the corresponding correlation coefficients. Every square root of each corresponding AVE exceeded the corresponding correlation coefficients, as shown in Table 3.

Table 3. Discriminant Validity

	PE	CON	PR	TR	IU
Personalization	**0.902**				
Connectivity	0.710	**0.917**			
Privacy risk	-0.106	-0.096	**0.949**		
Time Risk	-0.313	-0.356	0.433	**0.878**	
Intention to Use	0.549	0.577	-0.279	-0.423	**0.925**

PE: Personalization, **CON:** Connectivity, **PR:** Privacy risk, **TR:** Time risk, **IU:** Intention to use

Perceived benefits and perceived costs were measured as second-order factors. Perceived benefits were empirically validated as a second-order construct with two first-order reflective indicators—personalization and connectivity. Perceived costs were also empirically validated with two first-order reflective indicators—privacy risk and time risk. All path values between perceived benefits and perceive risk and each first-order constructs were significant, with values ranging from 0.690 to 0.905, which exceeded the required minimum of 0.50 (Fig. 5).

5.2 Hypothesis Testing

We analyzed our research model using the PLS method. Figure 4 presents the path coefficients summarization of the relationships in the structural model. As expected, compared with the no option condition, a linkage option (β = -0.356, $p < 0.001$), permeability option (β = -0.205, $p < 0.01$) and ownership option (β = -0.162, $p < 0.05$) had significantly negative effects on perceived benefits providing support for H1, H3, and H5. As articulated by H2 and H4, compared with no option, a linkage option (β = 0.276, $p < 0.01$) and permeability option (β = 0.238, $p < 0.05$) significantly increased perceived costs. The results validated the hypotheses. An ownership option also increased perceived costs compared with no option, it was not statistically significant (β = 0.116, $p > 0.05$). Thus, H6 was not supported. In support of H7 and H8, the perceived benefits positively influenced intention to use (β = 0.522, $p < 0.001$) and perceived cost was found to negatively influence intention to use smart home services (β = -0.263, $p < 0.001$). The R^2 of perceived benefits and perceived costs were 0.087 and 0.064, simultaneously. This is because dependent variables were dummy variables not continuous variables.

Finally, the R^2 of intention to user was 0.433

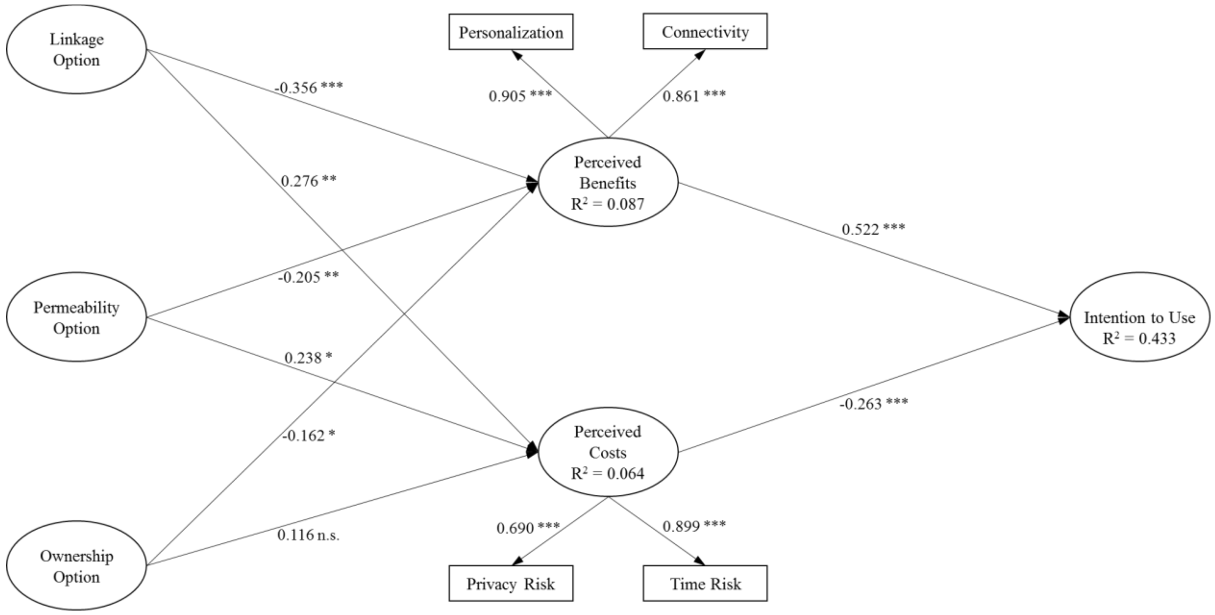

Linkage Option
Personalization
Connectivity
-0.356 ***
0.905 ***
0.861 ***
0.276 **
Perceived Benefits R² = 0.087
0.522 ***
-0.205 **
Permeability Option
Intention to Use R² = 0.433
0.238 *
-0.263 ***
-0.162 *
Perceived Costs R² = 0.064
0.690 ***
0.899 ***
0.116 n.s.
Ownership Option
Privacy Risk
Time Risk

Figure 4. Results of Research Model

5.3 Supplementary Analysis on the Effect of Smart Home Service Options

MANOVA was additionally conducted to compare the effects of the four service options on each first-order indicator of perceived benefits and perceived costs. First, we found that the types of control had a main effect on personalization ($F_{(3,331)} = 7.673$, $p < 0.001$) and connectivity ($F_{(3,331)} = 10.004$, $p < 0.001$) and participants expected that using any kinds of option would reduce the level of personalization and connectivity (Fig. 5). A linkage option, sharing information with neighborhoods, decreased the personalization and connectivity to its lowest level, followed by permeability and ownership options.

Second, the types of options have the main effect on security risk and time risk (Figure 6). Participants expected that using the services options would reduce the level of security risks ($F_{(3,331)} = 8.629$, $p < 0.001$); and an ownership option, the controlling of service provider rights, decreased the security risk to its lowest level, followed by a permeability option. However, linkage options had a similar effect to no option. In the case of time risk, participants expected that using smart home service options would induce the level of time risk ($F_{(3,331)} = 12.724$, $p < 0.001$). A linkage option increased the time risk to its highest level. However, there was no significant difference between three service options.

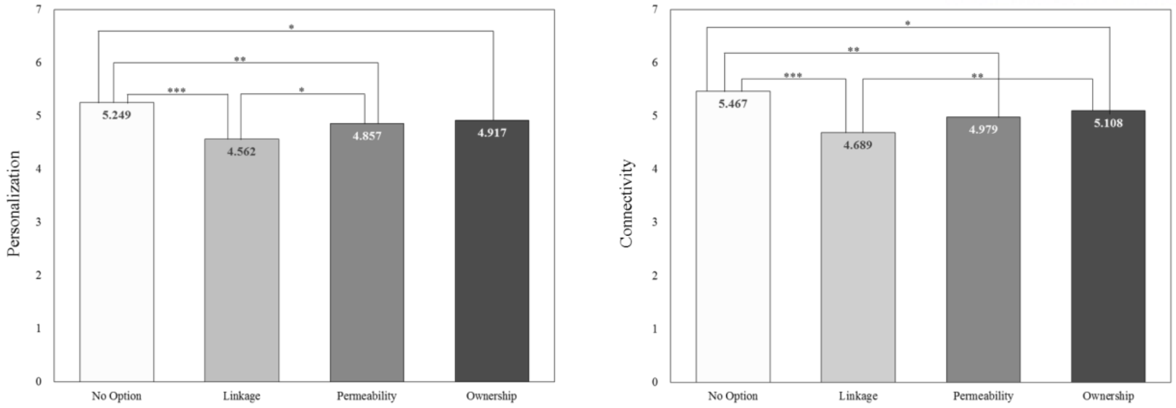


Figure 5. Effects of Smart Home Service Options on Perceived Benefits

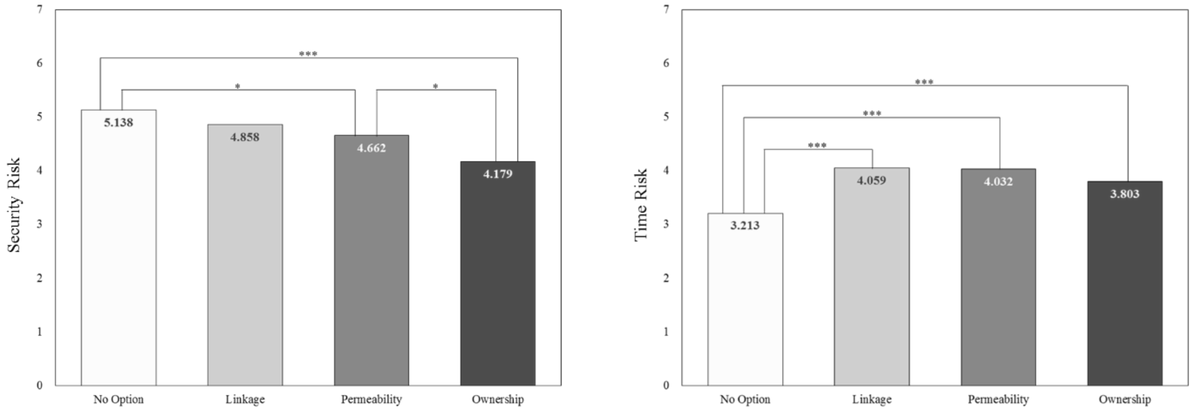


Figure 6. Effects of Smart Home Service Options on Perceived Risks

VI. Discussion

The negative effect of a linkage option on perceived benefits suggest that people consider social risks more than social benefits. Previous research indicated that the more sensitive the information shared with friends on SNS is, the more social risks, such as face risk and relational risk, increaesd (Lee et al., 2013). Permeability and ownership options also decreased perceived benefits. Prior research denoted that the degree of perceived benefits is affected by the sensitivity of information (Lee et al., 2013). People tend to expect more perceived benefits when they provide personal information with higher sensitivity. However, permeability and ownership options reduce the information sensitivity by eliminating accuracy of information and controlling the rights of service providers. As a result, permeability and ownership options had negative effects on both personalization and connectivity. In the aspects of perceived benefits, a linkage option reduced both personalization and connectivity the most. It suggests that smart home security information is particularly vulnerable to social risk.

Linkage and permeability options had positive effects on perceived costs, as we anticipated. It is because sharing personal information with others is a potential risk of control or loss of personal information due to vulnerabilities to loss caused by disclosure (Li et al., 2011). However, in the case of the ownership option, the effect on perceived costs was not significant. It seems to be due to the fact that the privacy risk had decreased and the time risk had increased, offsetting each other. Through supplementary analysis, the study demonstrated that both permeability and ownership options decreased privacy risk.

The results support the theory that people consider perceived benefits and perceived costs simultaneously. While perceived benefits had positive effects on intention to use smart home security services, perceived costs had negative impacts on intention to use. In particular, perceived benefits are more influential than perceived costs. This means that when deciding whether to use a smart home security service, users consider perceived benefits more. Previous research regarding personalization-privacy paradox showed that the personalization aspect was more prominent than the risk aspect in eliciting more information disclosure from users in an online context (Awad et al., 2006). The results of this study were consistent with previous studies in that perceived benefits have more impact on intention than perceived costs.

ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

VII. Implications, Limitations, Future Research, and Conclusions

7.1 Theoretical Implication

This research contributes to the field of smart home research. First, this study identified the users' perception of smart home using communication privacy management theory. We successfully introduced communication privacy management theory to the smart home context. In particular, one of the key issues of communication privacy management theory is privacy rules to control personal information. By successfully adapting communication privacy management theory to the smart home context, this research extends IoT research, as well as smart home research.

Second, this research showed that both perceived benefits and perceived costs have impacts on users' behavioral intentions. The effects of perceived benefits and perceived costs on intention to use smart home security services are consistent with the privacy calculus theory, suggesting perceived benefits increase intention to use and perceived costs decrease intention to use. Especially, in the smart home security context, people tend to consider perceived benefits more than perceived costs. By successfully applying privacy calculus theory to smart home services, this study suggested that the benefits and cost mechanisms can be applied to general smart home context.

Third, most previous smart home research have been qualitative studies and focused on seniors or the disabled. This study is nearly the first study that empirically approaches the study of smart homes for the general population. Also this study produced unique results that distinguished SNS contexts and mobile promotion contexts using communication privacy management theory and privacy calculus theory. Therefore, this study has notable theoretical significance as the cornerstone of the smart home context.

7.2 Practical Implication

This study provides guidelines for smart home service providers. The results showed that when smart home service options are used, perceived benefits decrease and perceived costs increase. It means that no option is the best. It is important to find a way to ensure that people are providing precise information. In particular, perceived benefits had more impact on intention to use smart home services than perceived costs. Therefore, service providers should strive to provide more personalized services. To increase connectivity with users, real-time feedback is also important. With enhanced sophisticated smart home services, service providers should adopt measures to not only reduce fears of privacy risk but also to improve confidence in their privacy protection.

Among the three service options, when an ownership option was used, the perceived benefit was highest. Essentially, when an ownership option was used, participants expected the lowest level of privacy risk. Therefore, it may be necessary to state the rights of smart home providers and how they control users' personal information. Otherwise, as in the case of a linkage option, the level of perceived benefits was the lowest and the level of perceived costs was the highest. Therefore, rather than additionally sharing personal information with neighborhoods, it is better for service providers to provide services based on individuals' user data.

To reduce the perceived costs, it seems likely that time risk should be decreased. According to the results, time risk affected perceived costs more than privacy risk. It means that when using additional options in smart home security services, people may consider extra time and effort more than disclosing their personal information. Prior research about information technology and switching costs explained that the introduction of gradual changes can lowers switching costs (Forman & Chen, 2006). Therefore when users adopt smart home services, service providers need to give guidelines gradually and steadily to reduce switching costs, such as additional time and effort.

7.3 Limitations and Future Research

This study has several limitations that suggest possibilities for further research. First, this research only focused on home security services, but future smart home services may evolve to focus more on energy management and lifestyle support. User perception of smart homes may vary depending on the service types. Therefore, further research is necessary to examine user perceptions of smart homes according to the service types.

The second limitation is that we measured intention to use smart home services as a dependent variable. As the number of smart home users increases, it is necessary to conduct experiments on actual users. The results of the study showed that the smart home service options decreased perceived benefits and increased perceived costs. This is because before using high-technology services, functional aspects or merits are generally highlighted; but when participants were offered smart home service options to protect their personal information, they should have been perceived more strongly as a risk. If this study becomes available to actual users, the results may be changed. Therefore, it is necessary to conduct research on actual users.

The third limitation is that of the perceived risks, this study measured only security risk and time risk. However, there will be more types of perceived risks that can be measured. In particular, when using new high-tech services, monetary risk is very important. In addition, there are other ways to measure the perception of users in regard to perceived risks facets, such as performance, social, financial, and psychological risks. Therefore, if a more diverse risk aspect is considered in the future study, it will be even more remarkable research.

The last limitation is that, in this study, it is assumed that the smart home service options can be set exclusively to investigate the effects of each option. However, when people use the options in real life, they can set the service options simultaneously. Therefore, it is necessary to consider their interactions. For example, when linkage and permeability options are set, or when all options are considered at the same time, users' perceptions will be different. In the future research, if the interaction effects are also considered, it will be a more notable study.

7.4 Conclusion

This study addressed an important gap in research in terms of understanding user perceptions of perceived benefits and perceived costs influencing the intention to use smart home security services, according to the types of service options. The empirical approach to perceptions of smart home services sheds light on how people perceive the benefits that smart home services offer. The extended privacy rules, introduced by the communication privacy management theory, can be adopted to explain users' behavioral intentions for smart home services.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 2*(2005), 24-30.

Adomavicius, G., & Tuzhilin, A. (2005). Personalization technologies: a process-oriented perspective. *Communications of the ACM, 48*(10), 83-90.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13-28.

Balaji, M. S., Khong, K. W., & Chong, A. Y. L. (2016). Determinants of negative word-of-mouth communication using social networking sites. *Information & Management, 53*(4), 528-540.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy, 63*, 363-374.

Bierhoff, I., van Berlo, A., Abascal, J., Allen, B., Civit, A., Fellbaum, K., Kristiansson, K. (2007). Smart home environment. *Towards an inclusive future: Imapact and wider potential of informational and communication technologies.*

Briere, D. (2011). *Smart homes for dummies*: John Wiley & Sons.

Chen, L. S.-L. (2010). The impact of perceived costs, intangibility and consumer characteristics on online game playing. *Computers in Human Behavior, 26*(6), 1607-1613.

Chen, P. Y., & Forman, C. (2006). *Switching costs, network effects, and buyer behavior in IT markets*. Working Paper, Georgia Institute of Technology, Atlanta, GA.

Chen, P. Y., & Hitt, L. M. (2006). Information technology and switching costs. *Handbook on Economics and Information Systems, 1*, 437-470.

Choi, S. (2016). The flipside of ubiquitous connectivity enabled by smartphone-based social networking service: Social presence and privacy concern. *Computers in Human Behavior, 65*, 325-333.

Chun, H., Lee, H., & Kim, D. (2012). The integrated model of smartphone adoption: Hedonic and utilitarian value perceptions of smartphones among Korean college students. *Cyberpsychology, Behavior, and Social Networking, 15*(9), 473-479.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115.

Demiris, G., & Hensel, B. K. (2008). Technologies for an aging society: a systematic review of “smart home” applications. *Yearb Med Inform, 3*, 33-40.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Ding, D., & Gebel, K. (2012). Built environment, physical activity, and obesity: what have we learned from reviewing the literature? *Health & place, 18*(1), 100-105.

Eriksson, H., & Timpka, T. (2002). The potential of smart homes for injury prevention among the elderly. *Injury control and safety promotion, 9*(2), 127-131.

Farooq, M., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(7), 1-6.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived costs facets perspective. *International journal of human-computer studies, 59*(4), 451-474.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660.

Hair, J.F., Ringle, C.M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *The Journal of Marketing Theory and Practice, 19*(2), 139-152.

Jeong, K.-A., Salvendy, G., & Proctor, R. W. (2010). Smart home design and operation preferences of Americans and Koreans. *Ergonomics, 53*(5), 636-660.

Ji, P., & Lieber, P. S. (2010). Am I safe? Exploring relationships between primary territories and online privacy. *Journal of Internet Commerce, 9*(1), 3-22.

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies, 71*(9), 862-877.

Lee, Y. K., Park, J. H., Chung, N., & Blakeney, A. (2012). A unified perspective on the factors influencing usage intention toward mobile financial services. *Journal of Business Research, 65*(11), 1590-1599.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434-445.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.

Nepomuceno, M. V., Laroche, M., & Richard, M. O. (2014). How to reduce perceived costs when buying online: The interactions between intangibility, product knowledge, brand familiarity, privacy and security concerns. *Journal of Retailing and Consumer Services, 21*(4), 619-629.

Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will self-disclose. *Personality and Social Psychology Review, 4*(2), 174-185.

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review, 2*(3), 175-196.

Pi, S.-M., Liao, H.-L., Liu, S.-H., & Hsieh, C.-Y. (2010). The effects of user perception of value on use of blog services. *Social Behavior and Personality, 38*(8), 1029-1040.

Seo, D. W., Kim, H., Kim, J. S., & Lee, J. Y. (2016). Hybrid reality-based user experience and evaluation of a context-aware smart home. *Computers in Industry*, *76*, 11-23.

Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications, 13*(5), 305-319.

Sherry, J. F., McGrath, M. A., & Levy, S. J. (1993). The dark side of the gift. *Journal of Business Research, 28*(3), 225-244.

Shih, D.-H., Hsu, S.-F., Yen, D. C., & Lin, C.-C. (2012). Exploring the individual's behavior on self-disclosure online. *International Journal of Human-Computer Interaction, 28*(10), 627-645.

Shmargad, Y., & Watts, J. K. (2016). When online visibility deters social interaction: The case of digital gifts. *Journal of Interactive Marketing, 36*, 1-14.

Swan, M. (2012). Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator Networks, 1*(3), 217-253.

Thin, N., Taylor, S., Bremner, S., Emmanuel, A., Hounsome, N., Williams, N., & Knowles, C. (2015). Randomized clinical trial of sacral versus percutaneous tibial nerve stimulation in patients with faecal incontinence. *British Journal of Surgery, 102*(4), 349-358.

Tojib, D., & Tsarenko, Y. (2012). Post-adoption modeling of advanced mobile service use. *Journal of*

Business Research, 65(7), 922-928.

Verma, A., Tiwari, M. K., & Mishra, N. (2011). Minimizing time risk in on-line bidding: An adaptive information retrieval based approach. *Expert Systems with Applications*, *38*(4), 3679-3689.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531-542.

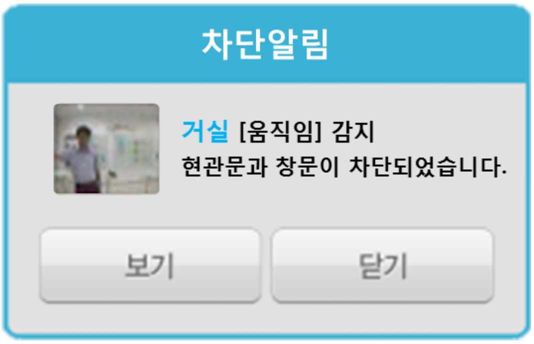
Wooten, D. B. (2000). Qualitative steps toward an expanded model of anxiety in gift-giving. *Journal of Consumer Research, 27*(1), 84-95.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135-174.

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce, 16*(4), 53-90.

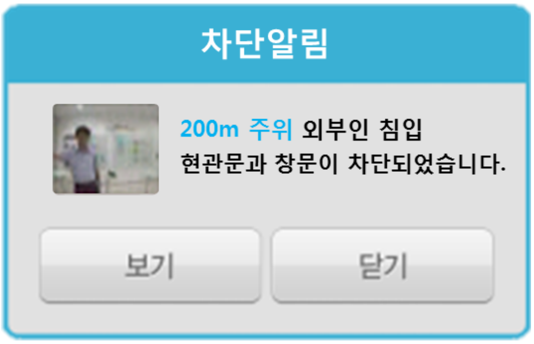
[Appendix] Figures of Manipulation


차단알림

거실 [움직임] 감지
현관문과 창문이 차단되었습니다.

If external intrusion is detected, in the living room of house, security services provider automatically lock the doors and windows.

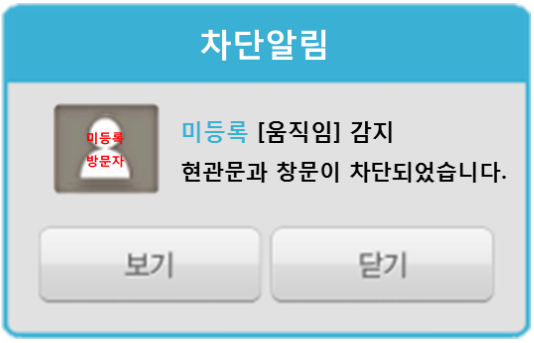
No smart home service option


차단알림

200m 주위 외부인 침입
현관문과 창문이 차단되었습니다.

If a thief breaks into a neighboring house, to prevent other accidents, the security services provider automatically locked doors and windows.

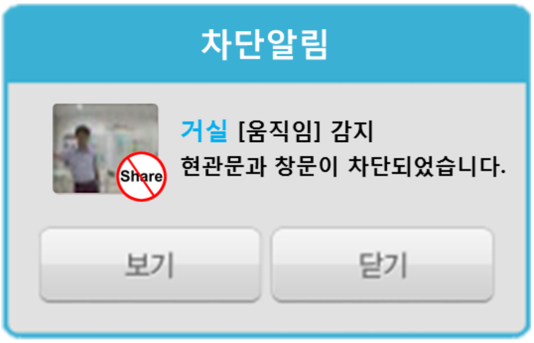
Linkage smart home service option


차단알림

미등록 [움직임] 감지
현관문과 창문이 차단되었습니다.

The provided information to the service provider only about whether the person is registered rather than precise information, such as a picture.

Permeability smart home service


차단알림

거실 [움직임] 감지
현관문과 창문이 차단되었습니다.

Security service providers who receive users' personal information just can see the information, they cannot modify or share with other service providers

Ownership smart home service option