ASIA MARKETING JOURNAL

ASIA MARKETING JOURNAL

Volume 24 | Issue 1 Article 4

May 2022

The Impact of Privacy Control on Users' Intention to Use Smart Home Internet of Things (IoT) Services

Mingyung Kim
SK Inc., Korea, ming_kim@sk.com

Bo Reum Choi
Business School, University of Seoul, Korea, bchoi@uos.ac.kr

Recommended Citation
Kim, Mingyung and Choi, Bo Reum (2022) "The Impact of Privacy Control on Users' Intention to Use Smart Home Internet of Things (IoT) Services," *Asia Marketing Journal*: Vol. 24 : Iss. 1 , Article 4.
Available at: https://doi.org/10.53728/2765-6500.1586

The Impact of Privacy Control on Users' Intention to Use Smart Home Internet of Things (IoT) Services

Mingyung Kim [a], Bo Reum Choi [b,*]

[a] SK Inc., Gyeonggi, South Korea
[b] Business School, University of Seoul, Seoul, South Korea

Abstract

Despite the diverse benefits of smart home Internet of Things (IoT) services, the biggest obstacle to the actual usage of those services is concern about privacy. However, little research has investigated the impact of privacy control on users' intention to use smart home services. Based on communication privacy management theory and privacy calculus theory, this study investigates how privacy control options affect users' perceived benefits and costs and how those perceptions affect individuals' intentions to use smart home services by conducting an experiment. Our results showed that smart home privacy control options decreased perceived benefits and increased perceived costs. The perceived benefits and costs significantly affected the intention to use smart home security services. More intriguingly, the effect of perceived benefit was found to be stronger than that of the expected cost. This research contributes to the field of IoT and smart home research and provides practitioners with notable guidelines.

Keywords: Smart home, Internet of things (IoT), Privacy rules, Privacy control

1. Introduction

As communication and information technologies have advanced, the Internet of Things (IoT) has changed the way people live. It encourages communication between devices and allows users to automate and control tasks in their daily lives. The number of connected devices, such as wearables, appliances, and automobiles, will exceed 38.6 billion worldwide by 2025 (Vailshery 2021). The IoT has a lot of applications in various fields, such as health monitoring systems, self-driven cars, IoT retail shops, and smart homes. In particular, revenue in the smart home market is expected to reach the US $126,111 million in 2022 and an annual growth rate is expected to be 13.30% (Statista, 2021). A smart home refers to automated services that can control and manage devices in the home locally or remotely (Jeong et al., 2010; Balta-Ozkan 2013). Integration of home-based networks into smart homes is expected to develop diverse beneficial properties. For example, users can control their home's lighting and thermostats via their smartphone without actually being home.

With the big opportunities of the IoT, however, concerns about security and privacy have been raised. When users disclose personal information to receive smart home services, unknown third parties may also be able to analyze their daily patterns. Researchers have identified IoT security and privacy as one of the most important aspects of IoT technologies (Schomakers, Biermann, and Ziefle 2021). A survey also showed that the biggest obstacle to investing in the IoT is concerned about the privacy and security aspects (Weissman, 2015). This is because there is the possibility that user information can be leaked by unauthorized third parties and be abused.

Although a few studies explain the importance of privacy issues (Farooq et al., 2015; McNealy and Mullis 2019; Zheng et al., 2018), 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

This paper is based on the first author's master's thesis.

Received 3 April 2022; accepted 14 April 2022.
Available online 6 May 2022.

* Corresponding author.
E-mail addresses: ming_kim@sk.com (M. Kim), bchoi@uos.ac.kr (B.R. Choi).

https://doi.org/10.53728/2765-6500.1586

or conceptual research focused on assisted living applications for elderly or disabled occupants (Demiris & Hensel, 2008; Ding & Gebel, 2012; Marikyan et al., 2019; Schomakers, Biermann, and Ziefle 2021). It is necessary to conduct empirical research from the perspective of regular individuals.

The purpose of this study is to investigate which smart home service privacy control option maximizes perceived benefits and minimizes perceived costs and how perceived benefits and costs affect users' intention to use smart home services. This study is based on two privacy-related theories: communication privacy management theory (Petronio 2001) and privacy calculus (Dinev & Hart, 2006), both are notable in the field of management information systems. 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. The privacy calculus theory is the most common approach to analyzing personal information disclosure behavior. By emphasizing the trade-off interrelation of self-disclosure, privacy calculus can be used to determine individuals' intentions to use smart home services.

2. Theoretical backgrounds

2.1. Communication privacy management theory and privacy rules

Communication privacy management (CPM) theory reveals a process in which users decide between sharing information with others and privacy concerns (McNealy and Mullis 2019). 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 (Li, 2012; Petronio, 2010). This theory allocates a level of perception to how people establish, manipulate, and exchange their private information. Petronio (2010) stated five core principles that determine how people disclose personal information. People manage their personal information by their privacy rules with the belief that they have the right to own and control their personal information (Petronio, 2010). When people share or give others access to their personal information, they become co-owners of that information (Petronio, 2010). 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, 2010). If the co-owners of personal information do not adhere to privacy rules, boundary turbulence may occur (Petronio, 2010).

According to the CPM theory (Petronio, 2010), 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 et al., 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 the 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 is 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. 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, the 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 privacy control options based on the three privacy rules of the CPM theory.

2.2. 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 cases, self-disclosure is a prerequisite to access additional services and is requested for these services to be personalized (Shih et al., 2012). When people reveal their personal information, however, they estimate the risks as well as the benefits (Acquisti & Grossklags,2005).

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 (Kim et al., 2019; Li et al., 2011) such as location-based services (Gutierrez et al., 2019; Xu et al., 2009; Xu et al., 2011; Zhao et al., 2012) and social media/commerce (Jozani et al., 2020; Sharma & Crossler, 2014). However, in a smart home context, there is little research that has adopted the privacy calculus theory to investigate disclosing personal information behaviors.

Perceived benefit is defined as the degree to which people believe that using the services would enhance their performance. Personalization and connectivity are considered perceived benefits that people most expect when using IoT services. Personalization is the ability to provide content and services that are customized to individuals based on information about their preferences and behaviors (Adomavicius, and 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, and Chung 2012; Tojib & Tsarenko, 2012). Connectivity is expected as a fundamental factor in the 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 devices" (Pi et al., 2010). It has commonly been identified with the multidimensional nature of the perceived cost construct (Featherman & Pavlou, 2003; Kim & Kim, 2014). Among various facets, privacy risk and time risk are considered perceived costs because these two can be applied to smart home services. Privacy risk is the possibility that your information is used without your permission (Featherman & Pavlou, 2003). Time risk is defined as the time consumers may lose by wasting time learning how to use a service (Featherman & Pavlou, 2003).

3. Hypotheses

A smart home provides diverse services based on an automated collection of devices and technologies working through home networking (Jeong et al., 2010). In particular, 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. If users set up a certain privacy control option, they can restrict the range of information they share, eliminate sensitive information, or control the rights of co-owners of personal information. Otherwise, i.e. no privacy control, they can share all personnel information related to their home with any service providers.

Linkage privacy control creates a collective boundary. When people share their information with diverse service providers, the possibility to receive various personalized services at any time they want increases. However, when they restrict sharing information with a small group of service providers, this possibility decreases. By sharing personal information with other people, people feel privacy risks (Acquisti & Grossklags,2005; Balaji, Khong, and Chong 2016; Kim & Kim, 2014) because the presence of third parties increases anxiety (Sherry, McGrath, and Levy 2013; Shmargad & Watts, 2016; Wooten, 2000). Determining information-sharing boundaries by setting linkage privacy control options decreases their anxiety. However, this privacy control requires some effort to decide who will be within this boundary. Users have to provide time and effort to search for information about service providers and compare their pros and cons with others. Thus, this will increase the time risk.

H1-1. Compared with no privacy control, a linkage privacy control will decrease a) personalization and b) connectivity.

H1-2. Compared with no privacy control, a linkage privacy control will a) decrease privacy risk and b) increase time risk.

A permeability privacy control eliminates sensitive information in advance and shares ambiguous information rather than precise information (Lee et al., 2013). According to previous research, perceived benefits are affected by information sensitivity (Omarzu, 2000). When people disclose sensitive information about their home, they anticipate personalized service and full access to the service. However, because a permeability privacy control obscures detailed information in advance, the sensitivity of information is reduced, so that people may anticipate a lower degree of perceived personalized services and connectivity. Meanwhile, 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 or open. 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, and Richard 2014). When using smart home security services, they have to determine what information to disclose and what information to conceal. This process requires additional time and effort to use the smart home services. Therefore, we can expect that a permeability privacy control will increase perceived time risk.

H2-1. Compared with no privacy control, a permeability privacy control will decrease a) personalization and b) connectivity.

H2-2. Compared with no privacy control, a permeability privacy control will a) decrease privacy risk and b) increase time risk.

An ownership privacy control is used to control the rights of co-owners of personal information who receive users' individual information (Petronio, 2010). The ownership privacy control prohibits service providers to share and reprocess users' private information and it leads to a decrease in perceived benefits. This is because they are not able to provide additional personalized services and the breadth of service is decreased. On the other hand, when users are informed of their rights in advance, people may feel less anxiety. Thus, privacy risks may decrease. Conversely, perceived time risk will increase because users need to monitor their service providers while using the smart home services to use an ownership privacy control. In particular, for the ownership privacy control, users constantly care for service providers to monitor the misuse of their personal information. As a result, using an ownership privacy control is considered a waste of time.

H3-1. Compared with no privacy control, an ownership privacy control will decrease a) personalization and b) connectivity.

H3-2. Compared with no privacy control, an ownership privacy control will a) decrease privacy risk and b) increase time risk.

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, and Chen 2016; Xu et al., 2011). Previous studies showed that the higher the uncertainty, the higher the perceived costs. People 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 use a smart home service.

H4-1. Perceived benefits positively affect intentions to use smart home services.

H4-2. Perceived costs negatively affect intentions to use smart home services.

4. Method

Embrain, the biggest online research agency with the largest consumer panel in Asia, was used to recruit 400 participants. 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.

The participants were provided with a scenario that described a situation in which they use each smart home service. The common situation was that sensors on doors and windows monitor movement in and near the home and collect information in real-time. If an external intrusion was detected and the user could check through a smartphone application by receiving an alarm notification. Using the CPM theory, four scenarios were manipulated including no privacy control and three privacy control options. No privacy control scenario stated if an external intrusion was detected, this information is automatically transmitted to any security service providers or police offices near home. The linkage privacy control scenario was manipulated by sharing this information only with the service providers or police offices the user selected in advance. The permeability privacy control was manipulated by concealing detailed information. For example, security providers can be noticed whether suspicious movements are incurred or not without comprehensive information about the movements. The ownership privacy control was manipulated by restricting the rights to control personal information. In this privacy control, the security service provider cannot reuse or modify the information or transmit this information to a third party. We tested the manipulation check for these privacy control options using independent t-tests and confirmed that the stimuli were valid.

Table 1. 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 the situation.	
Connectivity	CON1	I can access this smart home service information anywhere for the necessary service.	Chun et al. (2012)
	CON2	This smart home service allows me to use home security service anywhere at any time.	
	CON3	I can access this smart home service information at 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 risky.	
	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.	

After reading each scenario, the participants then responded to questions about their perception of the smart home service. 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 7 indicating “strongly agree” to 1 indicating “strongly disagree.” The measurement items are stated in Table 1 with the references.

5. Results

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 et al., 2011). We analyzed the data with SmartPLS3.0.

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.

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.

5.2. Hypothesis testing

MANOVA and t-test were conducted to compare the effects of the four privacy control options on each first-order indicator of perceived benefits (personalization and connectivity) and perceived costs (privacy risk and time risk). First, we found that the types of privacy options had a main effect on personalization (F (3,331) = 7.673, $p < 0.001$) and connectivity (F (3,331) = 10.004, $p < 0.001$) (Fig. 1). The results of the t-test showed that a linkage privacy control significantly decreased the personalization and connectivity to its lowest level ($p < 0.001$), followed by permeability ($p < 0.01$) and ownership ($p < 0.05$) privacy controls compared with no privacy control, supporting H1-1a & H1-1b, H2-1a & H2-1b, and H3-1a & H3-1b. Second, the types of privacy control options had the main effect on privacy risk and time risk (Fig. 2). Our results showed that the privacy control options reduced the level of privacy risks (F (3,331) = 8.629, $p < 0.001$); an ownership privacy control decreased the privacy risk to its lowest level ($p < 0.001$), followed by a permeability privacy control ($p < 0.05$), supporting H2-2a and H3-2a. However, the linkage privacy control did not significantly decrease privacy risk compared to no privacy control ($p > 0.05$), not supporting H1-2a. Our results also showed that the privacy control options increased the level of time risks (F (3,331) = 12.724, $p < 0.001$). A linkage privacy control increased the time risk to its highest level, followed

Table 2. Reliability and convergent validity.

Construct	Item	Factor	T-Value	Composite Reliability	AVE	Cronbach's *a*
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			

(Note: PE: Personalization, CON: Connectivity, PR: Privacy risk, TR: Time risk, IU: Intention to use).

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**

(Note: PE: Personalization, CON: Connectivity, PR: Privacy risk, TR: Time risk, IU: Intention to use).

by permeability ($p < 0.001$) and ownership ($p < 0.001$) privacy control options, supporting H1-2b, H2-2b, and H3-2b.

Second, the types of privacy control options had the main effect on privacy risk and time risk (Fig. 2). Our results showed that the privacy control options reduced the level of privacy risks (F (3,331) = 8.629, $p < 0.001$); an ownership privacy control decreased the privacy risk to its lowest level ($p < 0.001$), followed by a permeability privacy control ($p < 0.05$), supporting H2-2a and H3-2a. However, the linkage privacy control did not significantly decrease privacy risk compared to no privacy control ($p > 0.05$), not supporting H1-2a. Our results also showed that the privacy control options increased the level of time risks (F (3,331) = 12.724, $p < 0.001$). A linkage privacy control increased the time risk to its highest level, followed by permeability ($p < 0.001$) and ownership ($p < 0.001$) privacy control options, supporting H1-2b, H2-2b, and H3-2b.

To test the effect of perceived benefits and costs on intention to use smart home service, we used PLS. 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—

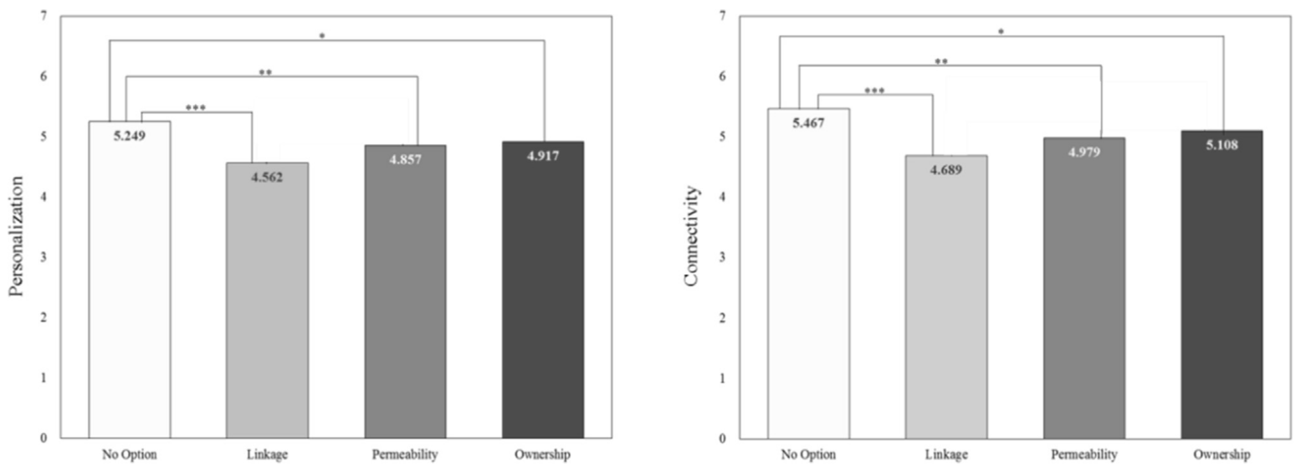

*Fig. 1. Effects of privacy control options on perceived benefits of smart home service. (Note: *p < 0.05, **p < 0.01, ***p < 0.001).*

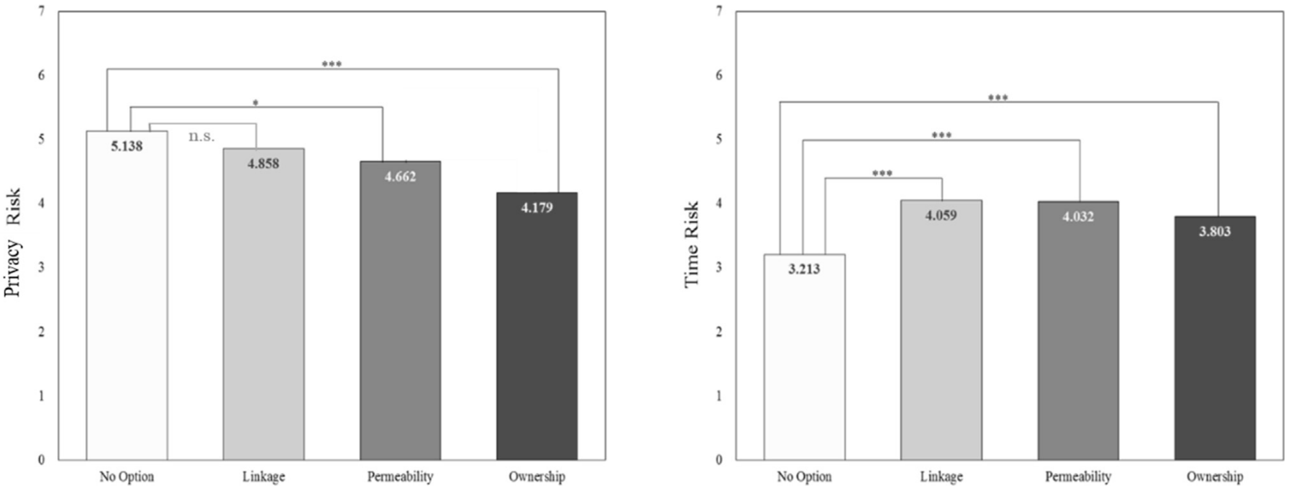

*Fig. 2. Effects of privacy control options on perceived risks of smart home service. (Note: *p < 0.05, ***p < 0.001, n.s. not significant).*

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 construct were significant, with values ranging from 0.690 to 0.905, which exceeded the required minimum of 0.50. The perceived benefits positively influenced intention to use (β = 0.522, p < 0.001), and the perceived cost was found to negatively influence intention to use smart home services (β = −0.263, p < 0.001). Thus, H4-1 and H4-2 were supported. Fig. 3 presents the path coefficients summarization of the relationships in the structural model.

6. Discussion

Our results showed that all three privacy control options decreased perceived benefits. Prior research denoted that the degree of perceived benefits is

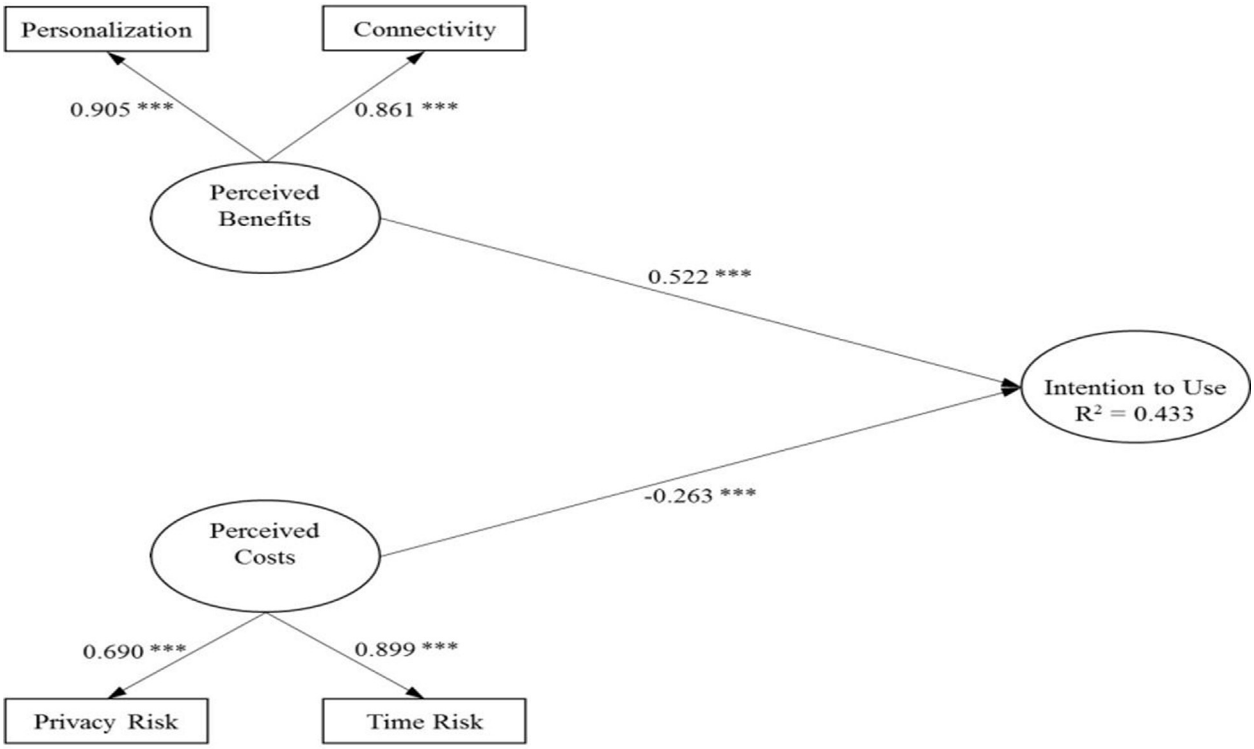

*Fig. 3. Effects of perceived benefits and costs on intention to use. (Note: ***p < 0.001).*

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, privacy control options reduce the information sensitivity by eliminating the accuracy of the information and controlling the rights of service providers. It is worthwhile to note that a linkage privacy control reduced both personalization and connectivity the most. This result suggests that creating a boundary by restricting sharing information with a small group of service providers particularly decreases the benefits of smart home service.

Our results also showed permeability and ownership privacy control options decreased privacy risk and increased time risk, as we anticipated. However, in the case of the linkage privacy control, the effect on privacy risk was not significant. It seems that smart home information is particularly vulnerable to social risk. The interesting result related to users' perceived cost is that an ownership privacy control reduced privacy risk the most and increased time risk the least. Thus, this suggests that the ownership privacy control is the most effective option to reduce users’ perceived risk.

Finally, our 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 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 service, users consider perceived benefits more. Previous research regarding the 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 & Krishnan, 2006). The results of this study were consistent with previous studies in that perceived benefits have more impact on intention than perceived costs.

7. Implications, limitations, and future research

7.1. Implications

This research contributes to the field of smart home research. First, this study identified the users’ perception of the 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. However, empirical research on communication privacy management theory is rare. By successfully adapting communication privacy management theory to the smart home context with empirical data for the general population, 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 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 the general smart home context.

This study provides guidelines for smart home service providers. Among the three service options, when an ownership option was used, the perceived benefits were highest and perceived costs were lowest. On the other hand, 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, it is more beneficial to users and service providers to clarify the rights of co-owners of personal information and how they control users’ personal information, rather than restricting a boundary to share their information.

In addition, perceived benefits had more impact on the 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.

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 privacy control options in smart home services, people may consider additional 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 lower switching costs (Chen & Forman, 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.

7.2. Limitations and future research suggestions

This study has several limitations that suggest possibilities for further research. First, this research only focused on home security services even though smart homes provide various services. Future research can consider diverse smart home services such as energy management and lifestyle support services. Users' perceptions and reactions to smart homes may vary depending on the service types. Thus, it will be interesting if future research can compare users' perceptions by comparing diverse smart home services.

The second limitation is that we did not conduct experiments with actual users. This study conducted a scenario-based experiment with possible smart home users. However, actual users' behavior and perceptions can be different from our results. This is because before using high-technology services, functional aspects or merits are generally highlighted. Moreover, users' characteristics such as technology readiness (Han & Park, 2016) and experience with customer support (Oh & Kim, 2022) can affect the results. Therefore, future studies need to investigate actual users of smart home services and the impact of their characteristics.

The third limitation is that this study only included security risk and time risk to measure perceived costs. However, there will be diverse types of perceived costs that can be measured. For example, in the case of new high-tech services, a monetary risk is a critical factor when users decide to use the services. In addition, there are other ways to measure the perception of users regarding perceived risks facets, such as performance, social, financial, and psychological risks. Therefore, future study needs to consider more diverse facets of perceived costs.

The last limitation is that this study assumes that the privacy control options can be set exclusively to investigate the effect of each option. However, when people set up privacy controls in real life, they can utilize multiple options simultaneously. For example, when linkage and permeability options are both selected, or when all options are considered at the same time, users' perceptions will be different. Thus, it will be meaningful if future research aims at these interactions.

Funding

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2020 S1A5A2A03041137).

References

Acquisti, Alessandro and Jens Grossklags (2005), “Privacy and rationality in individual decision making,” *IEEE Security & Privacy*, 3 (1), 26–33.

Adomavicius, Gediminas and Tuzhilin Alexander (2005), “Personalization technologies: A process-oriented perspective,” *Communications of the ACM*, 48 (10), 83–90.

Awad, Naveen Farag and Mayuram S. Krishnan (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 Kok Wei, and Chong Alain Yee Loong (2016), “Determinants of negative word-of-mouth communication using social networking sites,” *Information & Management*, 53 (4), 528–40.

Balta-Ozkan, Nazmiye, Rosemary Davidson, Martha Bicket, and Lorraine Whitmarsh (2013), “Social barriers to the adoption of smart homes,” *Energy Policy*, 63, 363–74.

Chen, Pei-Yu and Chris Forman (2006), “Can vendors influence switching costs and compatibility in an environment with open standards?” *MIS Quarterly*, 541–62.

Choi, Sujeong (2016), “The flipside of ubiquitous connectivity enabled by smartphone-based social networking service: Social presence and privacy concern,” *Computers in Human Behavior*, 65, 325–33.

Chun, Heasun, Hyunjoo Lee, and Daejoong Kim (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), 473–9.

Culnan, Mary J. and Pamela K. Armstrong (1999), “Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation,” *Organization Science*, 10 (1), 104–15.

Demiris, George and Brian K. Hensel (2008), “Technologies for an aging society: A systematic review of “smart home” applications,” *Yearbook of Medical Informatics*, 17 (1), 33–40.

Dinev, Tamara and Paul Hart (2006), “An extended privacy calculus model for E-commerce transactions,” *Information Systems Research*, 17 (1), 61–80.

Ding, Ding and Klaus Gebel (2012), “Built environment, physical activity, and obesity: What have we learned from reviewing the literature?” *Health & Place*, 18 (1), 100–5.

Farooq, M. Umar, Muhammad Waseem, Sadia Mazhar, Khairi Anjum, and Talha Kamal (2015), “A review on Internet of Things (IoT),” *International Journal of Computer Applications*, 113 (1), 1–7.

Featherman, Mauricio S. and Paul A. Pavlou (2003), “Predicting E-services adoption: A perceived risk facets perspective,” *International Journal of Human-Computer Studies*, 59 (4), 451–74.

Gutierrez, Anabel, Simon O'Leary, Nripendra P. Rana, Yogesh K. Dwivedi, and Tatiana Calle (2019), “Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor,” *Computers in Human Behavior*, 95, 295–306.

Hair, Joe F., Christian M. Ringle, and Marko Sarstedt (2011), “PLS-SEM: Indeed a silver bullet,” *Journal of Marketing Theory and Practice*, 19 (2), 139–52.

Han, Sang-Lin and Hyo-Ju Park (2016), “Effects of technology readiness on user perceptions and use intention of mobile social commerce,” *Asia Marketing Journal*, 18, 25–44.

Jeong, Kyeong-Ah, Gavriel Salvendy, and Robert W. Proctor (2010), “Smart home design and operation preferences of Americans and Koreans,” *Ergonomics*, 53 (5), 636–60.

Ji, Pan and Paul S. Lieber (2010), “Am I safe? Exploring relationships between primary territories and online privacy,” *Journal of Internet Commerce*, 9 (1), 3–22.

Jozani, Mohsen, Emmanuel Ayaburi, Myung Ko, and Kim-Kwang Raymond Choo (2020), "Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective," *Computers in Human Behavior*, 107, 106–260.

Kim, Ji Yoon and Sang Yong Kim (2014), "The effect of perceived risk, hedonic value, and self-construal on attitude toward mobile SNS," *Asia Marketing Journal*, 16 (1), 149–68.

Kim, Dongyeon, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn (2019), "Willingness to provide personal information: Perspective of privacy calculus in IoT services," *Computers in Human Behavior*, 92, 273–81.

Lee, Yong-Ki, Jong-Hyun Park, Namho Chung, and Alisha Blakeney (2012), "A unified perspective on the factors influencing usage intention toward mobile financial services," *Journal of Business Research*, 65 (11), 1590–9.

Lee, Haein, Hyejin Park, and Jinwoo Kim (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), 862–77.

Li, Yuan (2012), "Theories in online information privacy research: A critical review and an integrated framework," *Decision Support Systems*, 54 (1), 471–81.

Li, Han, Rathindra Sarathy, and Heng Xu (2011), "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors," *Decision Support Systems*, 51 (3), 434–45.

Marikyan, Davit, Savvas Papagiannidis, and Eleftherios Alamanos (2019), "A systematic review of the smart home literature: A user perspective," *Technological Forecasting and Social Change*, 138, 139–54.

McNealy, Jasmine and Mullis Michaela Devyn (2019), "Tea and turbulence: Communication privacy management theory and online celebrity gossip forums," *Computers in Human Behavior*, 92, 110–8.

Nepomuceno, Marcelo Vinhal, Michel Laroche, and Marie-Odile Richard (2014), "How to reduce perceived risk when buying online: The interactions between intangibility, product knowledge, brand familiarity, privacy and security concerns," *Journal of Retailing and Consumer Services*, 21 (4), 619–29.

Oh, Yun Kyung and Jung-Min Kim (2022), "What improves customer satisfaction in mobile banking apps? An application of text mining analysis," *Asia Marketing Journal*, 23 (4), 28–37.

Omarzu, Julia (2000), "A disclosure decision model: Determining how and when individuals will self-disclose," *Personality and Social Psychology Review*, 4 (2), 174–85.

Petronio, Sandra (2010), "Communication privacy management theory: What do we know about family privacy regulation?" *Journal of Family Theory & Review*, 2 (3), 175–96.

Pi, Shih-Ming, Hsiu-Li Liao, Su-Houn Liu, and Chia-Yu Hsieh (2010), "The effects of user perception of value on use of blog services," *Social Behavior and Personality: International Journal*, 38 (8), 1029–40.

Eva-Maria, Schomakers, Hannah Biermann, and Martina Ziefle (2021), "Users' preferences for smart home automation—investigating aspects of privacy and trust," *Telematics and Informatics*, 64, 101689.

Sharma, Shwadhin and Robert E. Crossler (2014), "Disclosing too much? situational factors affecting information disclosure in social commerce environment," *Electronic Commerce Research and Applications*, 13 (5), 305–19.

Sherry Jr, F. John, McGrath Mary Ann, and J. Levy Sidney (2013), "The dark side of the gift," *Journal of Business Research*, 28 (3), 225–44.

Shih, Dong-Her, Sheng-Fei Hsu, David C. Yen, and Chia-Chia Lin (2012), "Exploring the individual's behavior on self-disclosure online," *International Journal of Human-Computer Interaction*, 28 (10), 627–45.

Shmargad, Yotam and Jameson KM. Watts (2016), "When online visibility deters social interaction: The case of digital gifts," *Journal of Interactive Marketing*, 36, 1–14.

Statista. (2021), "Smart home report 2021. Statista digital market outlook - market report," (December 31), https://www.statista.com/study/42112/smart-home-report/.

Tojib, Dewi and Yelena Tsarenko (2012), "Post-adoption modeling of advanced mobile service use," *Journal of Business Research*, 65 (7), 922–8.

Vailshery and Lionel Sujay (2021), "IoT connected devices worldwide 2030," (January 22), https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/.

Wang, Tien, Duong Trong Danh, C. Charlie, and Chen. (2016), "Intention to disclose personal information via mobile applications: A privacy calculus perspective," *International Journal of Information Management*, 36 (4), 531–42.

Weissman, Cale Guthrie (2015), "Internet of Things survey results: IoT adoption is already significant," But Security Worries Persist. January 14 https://www.businessinsider.com/bi-intelligence-iot-survey-businesses-remain-wary-of-security-and-privacy-2015-1.

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

Xu, Heng, Xin Robert Luo, John M. Carroll, and Mary Beth Rosson (2011), "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decision Support Systems*, 51 (1), 42–52.

Xu, Heng, Hock-Hai Teo, Bernard CY. Tan, and Ritu Agarwal (2009), "The role of push-pull technology in privacy calculus: The case of location-based services," *Journal of Management Information Systems*, 26 (3), 135–74.

Zhao, Ling, Yaobin Lu, and Sumeet Gupta (2012), "Disclosure intention of location-related information in location-based social network services," *International Journal of Electronic Commerce*, 16 (4), 53–90.

Zheng, Serena, Noah Apthorpe, Marshini Chetty, and Nick Feamster (2018), "User perceptions of smart home IoT privacy," *Proceedings of the ACM on Human-Computer Interaction*, 2, 1–20. CSCW.