https://doi.org/10.5392/IJoC.2017.13.1.022

The Effects of Consumers' Perceived Privacy Control on Perceived Privacy Risk in Location-Based Services

Joohee Lee
Graduate School of Culture Technology
Korea Advanced Institute of Science and Technology (KAIST), Daejeon, 34141, Korea

Songmi Kim
Graduate School of Culture Technology
Korea Advanced Institute of Science and Technology (KAIST), Daejeon, 34141, Korea

Wonjoon Kim
School of Business and Technology Management
Korea Advanced Institute of Science and Technology (KAIST), Daejeon, 34141, Korea

ABSTRACT

The diffusion of advanced mobile technology has introduced new types of personal information or 'location data'. These new data mean new opportunities for businesses, such as location-based services (LBS), but have resulted in new consumer anxieties regarding disclosure of personal information. This study examines the effects of the consumers' perceived control over "time-and-place" information in location-aware services on their perceived privacy risk. A total of 270 respondents participated in this study. Conditions of perceived privacy control were operationalized over time-and-place information, in a 2x2 factorial design. Results indicate that the perceived control over time-and-place personal information is a significant predictor of perceived risk, and control assurances over time-and-place information enhances the perception of control, thus alleviating the perceived risk. In addition, the effect is much more significant when time and place were combined.

***Key words**: Privacy, Location-Aware Services, Perceived Risk, Perceived Control.*

1. INTRODUCTION

The advent of database systems, the Internet, and mobile platforms in particular have resulted in a switchover of a large portion of formerly private personal information to the public realm [1]. Consumers' personal information regarding age, family members, hobbies and/or purchasing behaviors are no longer exclusive to individuals because these personal data have become public records, as they are collected and used by many entities for a range of purposes, such as Internet or mobile marketing. In particular, firms and marketers collect a variety of personal information from consumers to use in their business strategies [2]. The advent of advanced wireless technology has introduced new types of personal information, including 'location data' and analyses of individual activity based on places and times [3]. Location-aware environments have created opportunities for businesses to more effectively exploit customer information. For instance, mobile commerce strategies involve targeted services that concentrate on customers' locations and push targeted marketing messages using Global Positioning Systems (GPS) [4]. In particular, the emerging ubiquitous field of location-based services (LBS) has injected considerable meaning into the practice of marketing in various ways, and location-sensing technologies have held a significant portion of certain ubiquitous environments, including ubiquitous ads and ubiquitous commerce fields. Location service providers detect consumers' location information, and firms can provide information that is tailored to individual consumers in their times of need [3].

According to Galanxhi-Janaqi and Nah [5], as firms learn the context of consumers' physical locations, they can match those consumers with relevant services and products. Moreover, marketers might expose consumers to targeted ads by tracking consumers' real-time locations and linking their data profiles at the household level [6]. Similarly, consumers also have recognized that personalized messages used in marketing that are based on consumers' specific locations and contexts are more useful than general messages [7]. For example, Krumm

* *Corresponding author, Email: songmi82@kaist.ac.kr*
Manuscript received Jan. 17, 2017; revised Feb. 06, 2017; accepted Feb. 13, 2017

[8] showed that location-sensitive ads are more effective than location-insensitive ads.

However, these characteristics of LBS have brought not only new opportunities for businesses but also anxiety for consumers with respect to disclosing or providing their location information. Unlike online virtual reality, a location-aware environment is based on and relevant to the everyday physical world [9]. Moreover, consumers' location information can be detected extensively, and each phase of detecting has its own uncertainties. Therefore, consumers perceive privacy risks when they understand that their personal information can be accessed, tracked continuously, and used without their knowing [10]. This is problematic because consumers' perceived privacy risk can influence not only message acceptance [11], which reduces advertising efficiency [12], but also intentions to adopt new technologies [13]-[15]. Therefore, a deeper understanding of consumers' perceived invasion of privacy by location-aware services is necessary to reduce their trepidation regarding unidentified risky situations and to enhance their intentions to adopt location-aware service.

In this regard, controlling perceptions regarding consumers' personal information is effective at alleviating their anxiety about the potential risks involved with unexpected privacy invasion. Spiekermann [16] defined "control perception" as an individual's belief that he/she can participate in deciding his/her range of detection in the electronic environment. This definition includes information controllability, which creates a sense of power and choice when individuals participate in decision making regarding the extent of how they will be scanned. Based on previous research, most consumers – even those who are relatively unconcerned about the ways in which marketers process collected data containing personal information [17]. Importantly, consumers' perceived control covers consumers' willingness to allow personal information to be transferred to third parties [18] and their intentions to adopt the services [19]. However, despite the importance of privacy matters in location-aware services, scant research has been undertaken on the preferences of control (i.e., how much or which part of their personal information consumers want to disclose) and on the relationship between perceived privacy control and privacy concerns. To fill this research gap, our study investigates the key factors of consumers' control perception over location-aware services, the amount of controllability, and the influence of these factors on perceived invasion of privacy.

The remainder of this paper is organized as follows. First, we discuss the previous literature on location-aware technology and services, consumers' perceived privacy risk, and perceived control related to the privacy debate. Then, we develop hypotheses. Next, we describe the methodology of our empirical study and present its results. Finally, we suggest directions for further research and conclude.

2. THEORETICAL BACKGROUND

2.1 Location-Aware Technology and Services

As part of technological progress, new computational features such as microphones, cameras, GPS, etc. are equipped in smartphones. These smart features allow companies to collect and assemble various types of personal information. With respect to the development of technology, urban sensing is a new sensing structure leveraging users as central components of a sensing network [20]. The GSM (global system for mobile) network, in particular, is considered as fundamental and essential to everyday life. These technologies allow for the real-time tracking of users' location data using mobile phones from distances of one hundred meters within cities to kilometers in more sparsely populated environments [21] and have enabled LBS.

The development of ubiquitous networks allows for continuous transactions and personalized communications between firms and their various related parties. The collection of consumers' real-time location data affects next-generation commerce: 'ubiquitous commerce (U-commerce)'. U-commerce provides more exclusive value than traditional (offline) commerce, e-commerce or m-commerce because it transcends temporal and spatial barriers [22]. In particular, RFID that enables identification from a distance and that supports a larger set of unique IDs automatically [23] is one of the most significant components to enable u-commerce business.

Moreover, a new type of marketing communication is possible with advances in mobile technologies. Location-aware technologies provide opportunities to advertisers' behavioral targeting based on users' temporal and spatial location data from wireless sensing [8]. Firms can provide consumers with location-sensitive messages with the help of location-aware technical capabilities [24]. For the first time, consumers can be reached with highly customized promotions and advertisements, based on their location at that moment [25].

These types of LBS have appeared as important components of the next generation of mobile commerce strategy [26], the market size of LBS has grown exponentially as these systems have become more available, accurate, and real-time and as various service opportunities have been established [22]. However, with every advance in technology, consumers' information becomes more extensively detected, and each phase of detecting became more ambiguous in a ubiquitous environment. Consequently, users have anxiety and general unease regarding the lack of control over their personal information in such an environment.

2.2 Consumers' Perceived Privacy Risk

The development of the Internet and mobile technology are considered the main reasons for changes in the ability of external factors regarding access to personal information [1]. Various types of personal information can be and are collected for diverse purposes [27], which can lead to serious threats to privacy if not properly managed [28]. In particular, the advanced mobile technologies associated with an individual's daily movement exacerbate the problem of privacy invasion because these technologies offer ubiquitous accessibility to unknown information collectors [29].

On the level of technology, pseudonym mode, which protects the consumer's real name and the confidentiality of anonymity through identity artifacts such as user ID and screen name [29], no longer ensures anonymity because the user's

location data may disclose his/her real-world identity from restricted or private places such as his/her house or office [30]. Thus, unsurprisingly, Cas [31] demonstrated that ubiquitous computing manifestations such as location-aware technology is currently considered the destroyers of all the central columns of current privacy protection.

For businesses, the problem is that perceived invasion of privacy may create significant barriers for message acceptance and advertising efficiency [11], even in terms of adopting location-aware services [13]. Xu [32] found that perceived privacy risk has a negative effect on behavioral intentions to adopt services in an LBS context. Therefore, it is important to reduce consumers' perceived risk related to their location information to increase their intentions to adopt location-aware services.

2.3 Privacy Control

In recent years, the definition of privacy has been actively debated, and these debates have mainly centered on the importance of advanced technologies and the greater number of possibilities for privacy invasion. Many studies have emphasized the consumers' right to controllability as a privacy concept [33]. For example, Stone, et al. [34] define privacy as the ability to control public access to personal information, and Bellman, et al. [35] define privacy concerns as anxiety regarding the invasion of one's privacy by external means over which the user has no control. Therefore, allowing users to control access to their personal information must be a main factor in privacy management.

Moreover, consumers' control perception about their personal information affects personalized online advertising click rates. The previous literature suggests that people are rarely concerned about personalized ads and reveal more information when enhancing their control settings [36], [18]. For example, Tucker [18] indicated that after the publicization of enhanced privacy control features, users clicked on personalized ads twice as much than before such publicization. Xu [32] also suggested that control assurance based on technology, self-regulation and government legislation might alleviate consumer concern.

Providing consumers with at least some control or allowing them to involve themselves in the subsequent dissemination of their personal information is required for firms' privacy management [18]. Even when the real risks related to providing information do not change at all, comparably weak control over the disclosure of private information can nonetheless reduce individuals' privacy concerns and increase their tendency to making disclosing sensitive personal information [36]. Thus, more specific and various technology-based control assurances are required than currently embodied in the relevant mechanisms. We expect that the extent of the right to exercise control over personal information more specifically and elaborately might influence the user's control assurance.

3. HYPOTHESES DEVELOPMENT

3.1 Control of Location- and Time-Aware Services

Several studies have examined the importance of control as a key pillar of privacy and insist that consumers are willing to expose more personal information after improving control assurance [18], [28], [32]. However, most previous studies showed only the tendency to share more information when users can control their information. For example, Xu [32] shows substantial variations of controllability between two groups: a control group and a non-control group. This author allows the first group to restrict the provider's access by turning off the mobile phone whenever users want to block access, whereas the second group is not permitted to turn off their phones. Tucker [18] also compared the advertising effectiveness before and after changes to privacy policies. Benisch et al. [37] showed significant variation in sharing preferences based on time of day and day of week, whereas Lederer, Mankoff, and Dey [38] demonstrated that users have specific information-sharing preferences when revealing or sharing their location data and that their preferences moderate the extent of their disclosure.

Therefore, further study is required to investigate consumers' perceptions when they are provided with more specific controllability regarding time and location data, i.e., how much or which part of their personal information they want to disclose. Hence, this study investigates the effects of the right to control both place and time on consumers' perceived control when they share their specific place and time information. In particular, we examine the effects of control assurances on consumers' perceived control and perceived risk when they can decide which place and time data they want to share with providers when the amount of information they reveal is fixed. Therefore, based on the above discussion, we posit the following hypotheses:

H1. The availability of location-based control assurance positively influences participants' perceived control.

H1a. The availability of time-based control assurance positively influences participants' perceived control.

H1b. The availability of place-based control assurance positively influences participants' perceived control.

H2. The availability of location-based control assurance negatively influences participants' perceived risk.

H2a. The availability of time-based control assurance negatively influences participants' perceived risk.

H2b. The availability of place-based control assurance negatively influences participants' perceived risk.

3.2 The Relationship between Perceived Control and Perceived Risk

The definition of 'privacy' in the academic literature is shown with respect to the relationship between control and risk in many cases. Studies on psychological risk also insist that risk perception is strongly influenced by costs and benefits, voluntariness, familiarity, and controllability [39], [40]. Malhotra et al. [28] investigated integrated dimensions of Internet users' information privacy concerns and suggest that

there is a direction from dispositional desire for information control to privacy risk. In addition, in an offline survey, Grag and Camp [41] investigated the dimensions of consumers' online perceived risk and identified controllability as one dimension of the nine risks. This literature thus suggests that control is an antecedent to risk because positive control perception generates lower estimates for negative consequences.

Building on these findings, we predict that, when consumers believe that services can be customized according to their needs and preferences, they will positively assess an innovation, i.e., a new service, because of the reduced perception of risk. Specifically, we hypothesize that perceived control over personal data is a predictor of perceived risk and that there is a similar relationship between privacy control perception and privacy risk perception when consumers provide location information.

H3. There is a negative relationship between participants' perceived control and perceived risk.

The research model for this study is depicted in Fig 1.

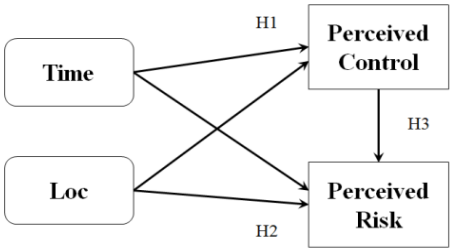

Fig. 1. Research model

4. METHOD

In this study, we investigate the effects of consumers' perceived control of the right to exercise authority over time and place information when sharing location information on consumers' perceived risk. Moreover, we examine the relationship between consumers' perceived control and perceived risk with regard to location-based services.

4.1 Procedure and Stimuli Design

An experimental design was conducted for testing causal relationships and enabling the manipulations of factors. We used a 2 (the right to exercise control over personal information regarding time; available vs. not available) x2 (the right to exercise control over personal information regarding location; available vs. not available) between-subject design (see Fig. 2). Between-subject design can reduce possible ordering effects that are problematic for within-subject experimental designs.

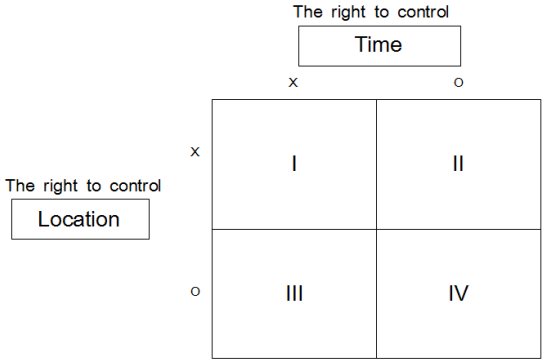

Fig. 2. Research design

We adopted the method of a scenario-based experiment including the fictitious study scenario developed in Cvrcek et al. [21]. The scenario-based method is generally used in experimental designs to manipulate different conditions of variables [42] and enables us to examine a possible future. Previous research related to location value made subjects believes sthat they were in a real situation of applying for an academic study on the mobility of people and that the participants in the fictitious study were selected through auction [42].

The fictitious study focused on tracking participants' mobile phone usage behavior through their locations over a month-long span. We are convinced that it is better to use an imaginary scenario to determine and prevent the danger of providing information that can be derived from a real situation. However, this setup can also lead to certain restrictions on the subsequent survey asking subjects about their perceived control, perceived risk, and demographic information. For this reason, we set up a slightly different situation in which subjects were requested to evaluate our fictitious forthcoming study but not to decide whether to participate in the fictitious study after reviewing the scenario.

4.2 Experimental Manipulation

Using four distinct scenarios, we manipulated the right to exercise control over personal information regarding time and place. Specifically, we suggested the following statements: 1) We plan to conduct mobile tracking to determine people's locational mobility over one month. 2) Subjects are to be asked to decide whether they want to be involved in a bid game to be selected as participants and for being rewarded in return for providing their location information. 3) Because of our limited budget, we will select those participants who bid the lowest amount of money. 4) We provide the right to exercise control over subjects' time-and-place personal information.

Specifically, we designed the experiment to assess perceived control when subjects are given partial control assurance as has been suggested in the literature and to increase the controllability slightly from that used in Brandimarte et al. [36]. Although the actual control function of LBS is to decide the place and time consumers want to share with providers, we manipulated the control with respect to not sharing information that participants do not want to reveal to enable decision making while noting the information to protect. Hence, four scenarios were suggested to subjects.

In all the scenarios, participants were tracked equally over sixteen hours and in four places every day. Significantly, we aim to prevent the differences in sensing control from becoming extreme among groups, which distinguishes this study from the previous literature [42]. Specifically, members of the first group were informed that they were randomly tracked for sixteen hours and in four places by researchers every day (scenario I). Those in the second group were informed that they were only randomly tracked in four places by researchers and could choose eight hours in which they would not be tracked (scenario II). Members of the third group were informed that they were randomly tracked for sixteen hours by researchers but could choose two places in which they would not be tracked (scenario III), and members of the fourth group were informed that they could choose eight hours and two places when and where they would not be tracked (scenario IV).

4.3 Measurement

The construct of perceived control was adopted from the control items on ubiquitous computing employed by Spiekermann [16] and Günther and Spiekermann [10]. Out of those items, we selected the following four. Next, we used the following measurement scale of perceived risk from Malhotra et al [28]. Detailed descriptions of these items, along with their original references, are provided in Table 1. All items were scored on a seven-point Likert scale (from 1 = "strongly disagree" to 7 = "strongly agree").

Table 1. Detailed Descriptions of the Scales

Variables	Scale items
Perceived control (Spiekermann 2005; Günther and Spiekermann 2005)	1) Information control, i.e., "I am always informed of whether and in what form the LBS tracks me" 2) Contingency, i.e., "I can determine for myself whether or not I'll interact with LBS" 3) Helplessness (reverse), i.e., "I can imagine that if LBS wants to scan me, LBS could do so without my permission" 4) Choice, i.e., "I have the final choice regarding whether or not I am being tracked."
Perceived risk (Malhotra et al. 2004)	1) It would be risky to give my information to online companies 2) There would be a high potential for loss associated with giving my information to online firms 3) There would be too much uncertainty associated with giving my information to online firms 4) Providing online firms with my information would involve many unexpected problems

4.4 Participants

A total of 270 respondents participated in this study including males (51.8%) and females (48.2%). The average age of the participants was 26.1 years. Table 2 depicts the subjects' demographic information. To assure independent responses from all the samples, we received all subjects' mobile phone numbers.

Table 2. Demographic Information of Subjects

Variable	Sample (%)
Gender	
Female	48.2
Male	51.8
Age	
20-24	52.5
25-29	42.2
30-34	4.2
35-39	1.2
Income (month)	
Less than $2,000	10.3
$2,000-$2,999	25.9
$3,000-$3,999	24.3
$4,000-$4,999	16.2
$5,000 or more	24.2
Mobility	
Several times a day	7.5
Once a day	20.7
Once a week	61.2
Once a month	11.7

Danezis, Lewis, and Anderson [43] suggested that the more frequently people move, the more sensitive they feel regarding control of their location information. Thus, we consider individual mobility as a control variable. In addition, Sheehan and Hoy [44] suggested that people's past experience with online service providers is one of the main reasons for trusting a provider with personal information online. Therefore, we also consider subjects' past experiences with LBS as a control variable. Participants' LBS experience is shown in Table 3.

Table 3. Subjects' Location-based Services Experiences

LBS Usage	Yes	203 (74%)
	No	70 (26%)
Frequency (per month)	average - 6.1 times	
Number of Services	average - 1.5 services	
Duration (months)	average - 8 months	

5. RESULTS

5.1 Control Checks and Manipulation Checks

We conducted control checks on LBS experience including LBS usage, duration, and frequency. Moreover, we conducted control checks on mobility and on the frequency of subjects' irregular movements, such as those associated with visiting friends, eating out, and travelling. ANOVA tests were performed to confirm that the random assignment of subjects to the four experimental conditions was successful. To check whether subjects properly understood each scenario, manipulation checks were asked for two items; time and place. In the questionnaire, we made inquiries regarding subjects' perceptions regarding their right to exercise control over their time-and-place information for each scenario. Subjects who did not correctly answer the above-mentioned questions were excluded from the data analyses, resulting in 218 valid data sets.

5.2 Factor Analysis

We performed a factor analysis to evaluate the reliability and validity of the constructs of perceived control and perceived risk. The reliability of all items is significant and is confirmed by checking that all items load on the intended construct. The Eigenvalue for perceived control is 4.69, and 39.08 percent of the variance is explained by this factor. The Eigenvalue for perceived risk is 2.53, and 21.05 percent of the variance is explained by this factor. Consequently, these two factors alone can explain a total of 60.13 percent of the variance. Cronbach's alpha coefficients are also used to evaluate the internal consistency or reliability of the constructs. As the Cronbach's alpha coefficients for perceived control (α = 0.856) and perceived risk (α = 0.873) exceed the threshold developed by Nunnally (1978) of 0.70, the measurements for the two constructs are highly reliable.

5.3 Perceived Control

We used a two-way ANOVA to test the significant differences in perceived control based on the availability of the right to exercise control over personal information regarding time and place. We used a 2 (time control; available vs. not available) x2 (place control; available vs. not available) between-subject experimental design. The main effect of time on perceived control is significant ($F(1, 217) = 88.47$, $p < 0.001$), and the main effect of place on perceived control is also significant ($F(1, 217) = 39.47$, $p < 0.001$). Table 4 depicts the results. Thus, H1 is supported.

Table 4. Means and Standard Deviations for Perceived Control

Time	Place	Perceived Control	
		Mean	Standard Deviation
Available	Available	4.42	0.93
	Not available	3.11	0.95
Not available	Available	2.71	0.94
	Not available	2.40	0.97

In addition, the results show that there is a significant interaction effect between the right to exercise control over personal information regarding time and the right to exercise control over personal information regarding place ($F(1, 217) = 15.58$, $p < 0.001$; see Fig. 3.). Thus, H1 was supported. Specifically, the difference between consumers' perceived control based on the right to exercise control over personal information regarding place is high when the right to have control over personal information regarding time is available than when it is not available. In addition, the right to have control over personal information regarding location improves perceived control, but perceived control significantly and substantially increases when the right to have control over personal information regarding place is combined with that regarding time.

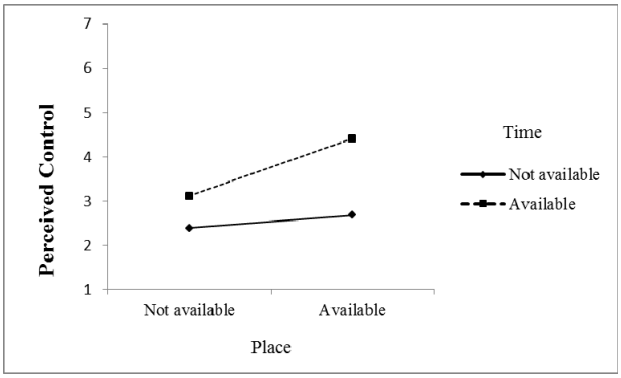

Fig. 3. Interaction of Place and Time on Perceived Control

5.4 Perceived Risk

We used a two-way ANOVA to assess the significant differences in perceived risk based on the right to exercise control over personal information regarding time and place. We again tested a 2 (time control; available vs. not available) x2 (place control; available vs. not available) between-subject experimental design. The main effect of time on perceived risk is significant ($F(1, 217) = 4.335$, $p < 0.05$), and the main effect of place on perceived risk is also significant ($F(1, 217) = 17.646$, $p < 0.001$). Table 5 depicts the results. Therefore, H2 is proven.

Table 5. Means and Standard Deviations for Perceived Risk

Time	Place	Perceived Control	
		Mean	Standard Deviation
Available	Available	4.54	1.14
	Not available	4.93	1.42
Not available	Available	4.57	1.21
	Not available	5.60	1.15

In addition, the results show that there is a significant interaction effect between the right to exercise control over personal information regarding time and that regarding place ($F(1, 217) = 3.449$, $p < 0.05$; see Fig. 4.). The right to exercise control over personal information regarding time itself reduces perceived risk, but perceived risk is significantly alleviated when the right to exercise control over personal information regarding time is combined with that regarding place. Moreover, the right to exercise control over personal information regarding place itself reduces perceived risk, but perceived risk decreases more when the right to have control over personal information regarding place is combined with that regarding time. The differences between consumers' perceived risk depending on the availability of control assurance is also significant. Notably, differences between consumers' perceived risk based on the right to exercise control over personal information regarding time are low when the right to have control over personal information regarding location is available.

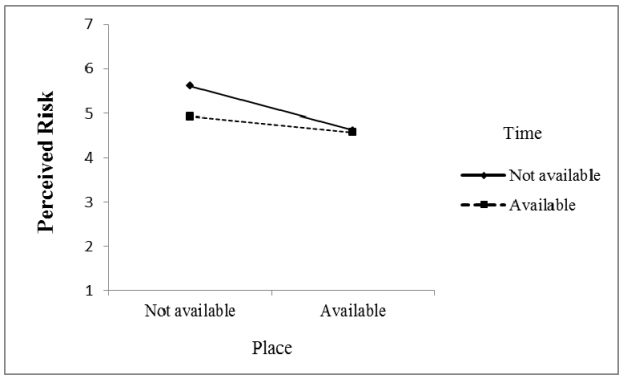

Fig. 4. Interaction of Place and Time on Perceived Risk

5.5 Perceived Control and Perceived Risk

We used a regression to evaluate the relationship between perceived control and perceived risk. As shown in Table 6, perceived control was a significant predictor for perceived risk. The coefficient of perceived control has a significantly negative correlation with perceived risk ($\beta = -.272$, $p < 0.001$). Moreover, the regression model that predicts perceived risk through perceived control is also significant ($F(1, 216) = 17.255$, $p < 0.001$; see Table 6.). Thus, H3 is accepted.

Table 6. Results of Regression

	Perceived Risk					
	Unstandardized Coefficients		Standardized Coefficients			
Model	*B*	Standard Error	*B*		t	Significance
(Constant)	5.827	0.241			24.219	0.000
Perceived Control	-0.294	0.071	-0.272		-4.154	0.000
		Sum of Squares	df	Mean Square	F	P
Regression		27.324	1	27.324	17.255	0.000
Residual		342.044	216	1.857		
Total		369.368	217			

Predictors: (Constant), Perceived Control

6. GENERAL DISCUSSION

6.1 Discussion

This study demonstrates the availability of the right to exercise control over personal time-and-place information to predict users' perceived control and risk when individuals provide their location information. We show the key factors of consumers' control perception for location-aware services, the amount of controllability and the influence of these factors on perceived invasion of privacy. We found that controlling time and pace data enhances control perception and alleviates risk perception, respectively. In addition, when consumers can control both variables, the effectiveness becomes much more significant. Specifically, although subjects are requested to provide the same amount of personal location data, their perceived control notably increased and perceived risk was significantly alleviated when they could decide which of these data they wanted to share with providers based on their time- and place-sharing preferences. Therefore, we reveal that partial control assurance helps increase control perception and reduce risk perception. Although it is enough to reflect on consumers' sharing preferences based on times and places singly, full control is better than partial control.

We also found that individuals' control perception is a significant predictor of risk perception when consumers are providing their personal information. As the prior research has shown [41], consumers' intentions to adopt privacy-sensitive services are affected by perceived privacy risk. Thus, alleviating consumers' privacy risk should be addressed by enhancing consumers' control perception. Specifically, when consumers believe that services can be customized based on consumer needs and preferences, they will positively assess the innovation because of the lower perception of risk.

6.2 Managerial Implications

The findings of our study have important managerial implications for practitioners. First, firms must offer fair information practices and must disclose procedures before collecting personal information from consumers. Consumers are tracked by providers not only with respect to their online behaviors but also with respect to their real-time offline identities. Specifically, whereas online privacy problems occur when information is collected from static computers, the information collection process of mobile devices is uncertain, and the range of detected data is extensive in a wireless sensing environment. Location is a type of information datum relatively more sensitive than information found online because the latter reveals real identity. Therefore, procedural justice must be established successfully by fair and operational information practices, such as collecting and subsequently using information when consumers provide personal information to firms in exchange for utility. In line with the findings of prior research [1], our results indicate that a privacy violation might be caused when consumers cannot decide the amount and depth of collected information. Consequently, we argue that the most important procedure is permission, which will greatly alleviate risk perception and subsequent potential negative outcomes [45].

Next, technological advancement allows providers to suggest personalized targeted messages to consumers. More personalized control assurance should therefore be offered to consumers to protect their information because a consumer's right to exercise control over personal information is an essential element of a reasonable implied social contract [46]. Consequently, this study argues that control and privacy management is necessary for marketing success. Marketers must realize that alleviating risk perception by means of permission and control assurance leads to enhancing service adoption and marketing executions.

6.3 Limitations and Avenues for Further Research

Further research can extend this study by taking individual differences into consideration and/or by using different amounts of control assurances which influence the privacy risks in LBS. First, further research can investigate the relationship between user mobility and privacy risk. Specifically, differences in people's sensitivity with respect to their locations might affect risk perception even when people do not move frequently. This subject is ripe for future research. Second, collecting location data may impact the perception of

privacy invasion. For example, the right to exercise control over personal information regarding time and place based on users' preferences is considered to be the most powerful assurance when sharing information not only with friends or families but also with advertisers and governments [37]. Thus, further research can extend the investigation to include the collection of location information and the different responses of consumers.

ACKNOWLEDGMENTS

This work has been prepared based on the master thesis of Joohee Lee who graduated from Graduate School of Culture Technology, KAIST in 2012.8. and was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2015-S1A3A-2046742).

REFERENCES

[1] N. Aldhafferi, C. Watson, and A.S.M. Sajeev, "Personal information privacy settings of online social networks and their suitability for mobile internet devices," International Journal of Security Privacy and Trust Management, vol. 2, no. 2, 2013, pp. 1-17.

[2] D. J. Solove, *The Digital Person: Technology and Privacy in the Information Age,* New York: New York University Press, 2004.

[3] P. K. Kannan, A. M. Chang, and A. B. Whinston, "Wireless commerce; Marketing issues and possibilities," Proceedings from 34th International Conference on System Sciences, p. 6.

[4] J. Wu and T. Hisa, "Developing E-Business Dynamic Capabilities: An Analysis of E-Commerce Innovation From I-, M-, To U-Commerce," Journal of Organizational Computing and Electronic Commerce, vol. 18, no. 2, 2008, pp. 95-111.

[5] H. Galanxhi-Janaqi and F. Nah, "U-commerce: Emerging Trends and Research Issues," Industrial Management & Data Systems, vol. 104, no. 9, 2004, pp. 744-755.

[6] C. E. Tucker, "The Economics of Advertising and Privacy," International Journal of Industrial Organization, vol. 30, no. 3, 2012, pp. 326-329.

[7] R. T. Watson, L. F. Pitt, P. Berthon, and G. M. Zinkhan, "U-Commerce: Expanding the Universe of Marketing," Journal of the Academy of Marketing Science, vol. 30, no. 4, 2002, pp. 333-347.

[8] J. Krumm, "Ubiquitous Advertising: The Killer Application for the 21st century," IEEE Pervasive Computing, vol. 10, no. 1, 2011, pp. 66-73.

[9] M. Weiser, "Some Computer Science Issues in Ubiquitous Computing," IEEE Computer, vol. 36, no. 7, 1993, p. 75.

[10] O. Günther and S. Spiekermann, "RFID and the Perception of Control: The Consumer's View," Communications of the ACM, vol. 48, no. 9, 2005, pp. 73-76.

[11] M. Johnson, S. Egelman, and S. M. Bellovin, "Facebook and privacy: It's complicated. Proceedings from SOUPS, '12 Proceedings of the eighth Symposium on Usable Privacy and Security, 2012, p. 9.

[12] D. A. Yorke and P. J. Kitchen, "Channel Flickers and Video Speeders," Journal of Advertising Research, vol. 25, no. 2, 1985, pp. 21-25.

[13] H. Li, R. Sarathy, and H. Xu, "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," Decision Support Systems, vol. 51, no. 3, 2011, pp. 434-445.

[14] D. H. Shin, "Ubiquitous Computing Acceptance Model: End User Concern about Security, Privacy and Risk," International Journal of Mobile Communications, vol. 8, no. 2, 2010, pp. 169-186.

[15] T. Zhou, "The Impact of Privacy Concern on User Adoption of Location-Based Services," Industrial Management & Data Systems, vol. 111, no. 2, 2011, pp. 212-226.

[16] S. Spiekermann, "Perceived control: Scales for privacy in ubiquitous computing," International Conference on User Modeling, 2005.

[17] J. Phelps, G. Nowak, and E. Ferrell, "Privacy Concerns and Consumer Willingness to Provide Personal Information," Journal of Public Policy & Marketing, vol. 19, no. 1, 2000, pp. 27-41.

[18] C. E. Tucker, "Social Networks, Personalized Advertising, and Privacy Controls," Journal of Marketing Research, vol. 51, no. 5, 2014, pp. 546-562.

[19] B. Suh and I. Han, "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce," International Journal of Electronic Commerce, vol. 7, no. 3, 2003, pp. 135-161.

[20] A. T. Campbell, S. B. Eisenman, N. D. Land, E. Miluzzo, and R. A. Peterson, "People-centric urban sensing (invited paper)," Proceedings from the Second ACM/IEEE International Conference on Wireless Internet, Boston, MA., 2006.

[21] D. Cvrcek, M. Kumpost, V. Matyas, and G. Danezis, "A study on the value of location privacy," Proceedings from Workshop on the Economics of Information Security Series (WEIS 2006) ACM, 2006, pp. 109-118.

[22] I. Junglas and R. Watson, "U-commerce: A conceptual extensions of e-commerce and m-commerce," Proceedings from International Conference on Information Systems, 2003, pp. 667-676.

[23] M. Ohkubo, K. Suzuki, and S. Kinoshita, "RFID privacy issues and technical challenges," Communications of the ACM, vol. 48, 2005.

[24] C. Ververidis and G. C. Polyzos, "Mobile Marketing using a location based service," Proceedings from 7th International Conference on Mobile Business, 2003.

[25] B. Kolmel and S. Alexakis. "Location Based Advertising," Proceedings from The First International Conference on Mobile Business, 2002.

[26] B. Rao and L. Minakakis, "Evolution of Mobile Location-Based Services," Communications of the ACM, vol. 46, no. 12, 2003, 2003, pp. 61-65.

[27] T. Dinev and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions," Information Systems Research, vol. 17, no. 1, 2006, pp. 61-80.

[28] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns(IUIPC): The Construct, The Scale, and a Causal Model," Information Systems Research, vol. 15, no. 1, 2004, pp. 336-355.
[29] Y. Chen, S. Wu, and X. Jiao, "Risk perception of individual suppliers in e-commerce transactions," Proceedings from SWS '09 1st IEEE Symposium on Web Society, pp. 194-199.
[30] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," Proceedings from 15th International Symposium on Advances in Geographic Information Systems ACM GIS, Article 39.
[31] J. Cas, "Privacy in Pervasive Computing Environments-A Contradiction in Terms?," IEEE Technology and Society Magazine, vol. 24, no. 1, 2005, pp. 24-33.
[32] H. Xu, "The effects of self-construal and perceived control on privacy concerns," Proceedings from Twenty Eighth International Conference on Information System, 2007, pp. 1-14.
[33] B. Rossler, *Privacies Philosophical Evaluations,* Stanford, CA: Stanford University Press, 2004.
[34] E. F. Stone, H. G. Gueutal, D. G. Gardner, and S. McClure, "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," Journal of Applied Psychology, vol. 68, no. 3, 1983, pp. 459-468.
[35] S. Bellman, E. J. Johnson, S. J., Kobrin, and G. L. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers," Information Society, vol. 20, no. 5, 2004, pp. 313-324.
[36] L. Brandimarte, A. Acquisti, and G. Loewenstein, "Misplaced confidences: Privacy and the control paradox," Proceedings from Workshop on the Economics of Information Security (WEIS), vol. 4, no. 3, 2013, p. 340.
[37] M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor, "Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs," Personal and Ubiquitous Computing, vol. 15, no. 7, 2011, pp. 679-694.
[38] S. Lederer, J. Mankoff, and A. K. Dey, "Who wants to know what when? Privacy preference determinants in ubiquitous computing," Chicago: ACM, pp. 724-725.
[39] P. Slovic, *The perception of risk. Risk, society, and policy series,* London, England: Earthscan Publications.
[40] J. A. Swaney, "Social economics and Risk Analysis," Review of Social Economy, vol. 53, no. 4, 1995, pp. 575-594.
[41] V. Grag and J. Camp, "End user perception of online risk under uncertainty," Proceedings from 45th Hawaii International Conference on System Science, 2012.
[42] H. Xu and H. H. Teo, "Alleviating consumers' privacy concerns in location based services: A psychological control perspective," Proceedings from International Conference on Information Systems, 2004.
[43] G. Danezis, S. Lewis, and R. Anderson, "How much is location privacy worth?," Proceedings from Fourth Workshop on the Economics of Information Security Series (WEIS 2005) ACM, 2005.
[44] K. B. Sheehan and M. G. Hoy, "Dimensions of Privacy Concern among Online Consumers," Journal of Public Policy & Marketing, vol. 19, no. 1, 2000, pp. 62-73.
[45] M. J. Culnan and P. K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," Organization Science, vol. 10, no. 1, 1999, pp. 104-115.
[46] M. J. Culnan, "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," MIS Quarterly, vol. 17, no. 3, 1993, pp. 341-364.

Joohee Lee
She received the B.S., in Business Administration from Kyung Hee University, Korea in 2010. She received her M.S. in Culture Technology from KAIST, Korea in 2012. Her main research interests include social media marketing and culture technology.

Songmi Kim
She received the B.S., M.S in Business Administration from Seoul National University, Korea in 2007, 2009 respectively. She received her Ph.D. in Culture Technology from KAIST, Korea in 2017. Her main research interests include social media marketing and culture technology.

Wonjoon Kim
He is an Associate professor at the School of Business and Technology Management, KAIST. He has been conducting and publishing researches on the strategic management of innovation. His current research interest also covers the changing nature of innovation, including technology and industry convergence, social network innovation, big data science as well as the changing nature of the process of entrepreneurship.