https://doi.org/10.14400/JDC.2017.15.12.265

Influence of Privacy Concerns on Intention to Use Location-based Services Based on Privacy Calculus Perspective

Jongki Kim
Dept. of Business Administration, College of Business, Pusan National University

프라이버시 계산 관점에서 위치기반서비스 이용의도에 대한 프라이버시 염려의 영향

김종기
부산대학교 경영대학 경영학과

Abstract As Location-based services on smartphone are getting more popular, users have more concern on exposing their location information. This study developed a research model to identify how smartphone users perceive on providing information pertaining to their location based on privacy calculus theory. 203 responses were analyzed with SmartPLS 2.0. The outcome of this research is quite interesting because conventional belief of privacy calculus perspective does not hold. The privacy calculus theory is based on assumption that human being is rational and decision to provide privacy information is determined by risk and benefit aspects. However, the result of this study is in accordance with behavioral economics perspective in which emotional judgment and behavioral judgement are affected by different factors.

Key Words : Smartphone, Privacy, Location-based Services, Privacy Calculus, Behavioral Economics

요 약 스마트폰의 위치기반서비스가 활발히 사용됨에 따라 사용자들이 자신의 위치정보의 노출에 대한 염려가 커지고 있다. 본 연구는 프라이버시 계산 이론에 기반하여 스마트폰 사용자들이 자신의 위치정보의 제공을 어떻게 받아들이는지 확인하고자 연구모형을 개발하였다. 대학생을 대상으로 수집한 데이터를 SmartPLS를 이용하여 분석한 결과 프라이버시 계산 관점의 기존 연구와는 다른 결과를 얻었다. 프라이버시 계산이론은 인간은 합리적인 존재이며, 위험과 효과 측면을 고려하여 프라이버시 정보의 제공을 결정한다고 본다. 본 연구의 결과는 프라이버시 염려는 위험에 유의하게 영향을 미치나, 사용의도는 효과에 의해서 유의하게 영향을 미쳤다. 이러한 결과는 감정적 판단과 행동적 판단이 서로 상이한 요인에 의해서 영향을 받는다는 행동경제학적 관점과 일치한다.

주제어 : 스마트폰, 프라이버시, 위치기반서비스, 프라이버시 계산, 행동경제학

1. Introduction

Today, smartphone has become one of the most important information and communication tools. Smartphone is commonly used by great portion of human beings in every corner of the world. The

* This study was supported by the Fund for Humanities & Social Studies at Pusan National University 2016.
Received 3 November 2017, Revised 1 December 2017
Accepted 20 December 2017, Published 28 December 2017
Corresponding Author: Jongki Kim (Pusan National University)
Email: jkkim1@pusan.ac.kr

ISSN: 1738-1916

percentages of smartphone usage in many countries were exceeded those of PC in 2014[1].

One of the most widely used smartphone applications is location-based services (LBS). According to a recent survey, 74 percent of smartphone owners used applications based on their location[2]. Users get directions from navigation applications. Social media users include location information in their posts.

While LBS provide promising business opportunities, they also raise serious concerns on information privacy. Some smartphone users decided not to use apps after they discovered how much personal information should be provided[3]. It posits great barriers on popular use of mobile apps based on LBS. Apple received a worldwide attention when it gathered location information of iPhone users without proper permission. Google also charged with same violation[4].

A study by Yankelovich Partners reported that 90% of its respondents felt that privacy was one of the most significant concerns about online shopping; it is rated more important than prices or return policies[5]. A study conducted by Hoffman and Novak[6] concluded that about 95% of the Internet users they surveyed were not willing to provide their personal information to the websites they used.

Nowadays, information communication technology provides valuable services and improve quality of life. LBS, one of the most commonly used ICT services, provides valuable mobile services, but at the same time it also generates significant privacy concerns. This study investigates how smartphone users perceive providing personal information pertaining to their location and eventually using LBS. The research model is based on privacy calculus theory. The results of this study would provide significant insights on how users perceive the opportunities and threats of privacy aspect of applications using LBS.

2. Literature Review

2.1 Location-Based Services

Smartphones are equipped with various sensing devices such as accelerometer, gyroscope, light sensor, proximity sensor, magnetometer, infrared sensor, and etc. LBS refer to the application services that provide various services based on device's location information. Location information is generated by GPS (Global Positioning System) sensor. LBS began with the development of GPS for the military use in 1970s. Nowadays, the advent of network technology enables use of GPS on WiFi and sensor network. Recent widespread use of smartphone provides opportunity for proliferation of LBS.

There are two types of research in IS on LBS; location-tracking services and position-aware services. Location-tracking services provide positional information about user's location to other than user himself or herself. On the other hand, location-aware services provide locational information to the actual user who is the information requester. That is, the main difference between two services is the recipient. The requesting individual of location-aware services is the recipient, but someone or something other than the user asks and gets location information in the case of location-tracking services[7].

2.2 Privacy and Privacy Concerns

Jourard[8] argued privacy as an outcome of people withholding certain information about their experiences from others. Information privacy is about "the ability of the individual to personally control information about one's self"[9]. Privacy concerns were to "stem from a variety of factors, including the individual's previous learning, cultural milieu, and physiological reactivity"[10].

In the context of e-commerce, privacy refers to the protection of personal information which is used for transaction. Invasion of privacy usually resulted in "the unauthorized collection, disclosure or other uses of

personal information as a result of online transactions"[11]. Prior research on privacy indicated that people are willing to disclose their personal information in return of monetary benefit based on the privacy calculus. The privacy calculus theory is a perspective that individuals assess whether to provide their personal information by evaluating negative consequences of providing their information and positive benefits of the services they use[12].

Many research indicated that privacy concerns affect the regulation to protect users' personal information, the users' trust belief, risk belief and the behavioral intention on the Internet. Information privacy concerns refer to an "individual's subjective views of fairness within the context of information privacy"[13]. Smith et al.[14] performed a series of studies to understand the complexity of perceived privacy concerns of Internet users. Their study designed to prove individuals' concerns about organizational information privacy practices and proposed a multidimensional scale, called concerns for information privacy (CFIP)[15].

Smith et al.[14] proposed four dimensions of CFIP; collection of personal information, secondary use of personal information, errors in personal information and improper access to personal information. First, concern for collection of personal information implies "the perception that extensive amount of personally identifiable data are being collected and stored in database"[14]. Internet users provide various kinds of personal information. Over time, the amount of information accumulated is getting bigger, which causes users to have great concerns on how they are used. Second type of concern is secondary use of personal information. It includes sharing privacy information with other parties who do not involve in the original transaction, or combining originally collected privacy information with other data such as demographic data to create profile of the owner of the personal information[14].

Third, concern on improper access means that "individuals' data are readily available to people not properly authorized to view or work with these data"[14]. Fourth, concern for errors implies that "protections against deliberate and accidental errors in personal data are inadequate"[14]. Many users consider that companies do not take appropriate measures to control information privacy problems. Although significant portion of the problems stem from deliberate action, problems caused by accidental errors cannot be ignored.

Concerns on privacy in LBS resulted in legal regulation control. In USA the Location Privacy Protection Act of 2012 was introduced to handle the transmission and sharing of location-based information. The bill encompasses the parties collecting data, the object data and its use of data. However, The bill does not cover the time span of holding the data, nor the data stored locally on the device[16].

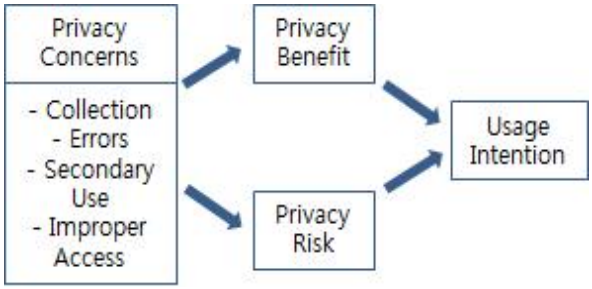
2.3 Privacy Calculus

Privacy calculus perspective assumes that users are rational decision-makers. That is, they make decisions to maximize their utility by balancing benefits and risks of conducting certain behavior. Dinev and Hart[17] proposed an extended privacy calculus model based on two main components of the TRA and TPB models. They proposed a research model to better understand the subtle balance between privacy risk beliefs and confidence beliefs which affect the intention to provide privacy information for conducting transactions on the Internet[17].

3. Research Model and Hypotheses

The research model proposed in this study is to identify users' intention to use LBS based on privacy calculus perspective as shown in [Fig. 1]. The model also includes that user's privacy concern affects his/her evaluation on benefit and risk of providing privacy

information. The privacy concerns are operationalized as discussed by Smith at al.[14], but it is measured as formative second-order construct as suggested by Stewart and Segars[18].



[Fig. 1] Research Model

<Table 1> describes measurement items of research constructs, which are based on prior research. Questionnaire is drawn from the measurement items and all measured by 5-point Likert-type scale.

<Table 1> Measurement Items

Item
Collection: 1) LBS asking for personal information 2) providing location information to LBS 3) location information collected on LBS 4) location information provided by users
Secondary Use: 1) using location information for any other reason 2) using location information for any other purpose without authorization 3) sharing location information with other parties 4) selling location information to other parties
Improper Access: 1) location information should be protected from improper accessing 2) preventing improper access to location information 3) taking better steps to make sure unauthorized people can not access location information 4) devoting more time and effort to preventing unauthorized access to location information
Errors: 1) storing location information accurately 2) ensuring the accuracy of location info. collected 3) aking better steps to make sure location information is accurate 4) devoting more time and effort to make sure location information is accurate
Benefit: 1) be safe to use LBS 2) getting location information in orderly fashion 3) handling location info. submitted appropriately 4) pursuing some policies related to location info.
Risk: 1) would cause some financial loss 2) would cause some privacy invasion 3) would cause some unexpected problems 4) trust in LBS would be lower
Usage Intention: 1) intend to use LBS which provide info. I wanted 2) intend to use LBS which can help my work 3) will use LBS that provide the info. I wanted 4) will use LBS which can ease my work

Malhotra et al.[15] argued that Internet-specific privacy concerns have a negative impact on trust-related beliefs. Those users who have a high degree of information privacy concerns tend to have low trusting beliefs. This observation is in congruence with TRA. The theory argues that individual characteristics affect intrinsic beliefs on trust[19]. First hypothesis is about the relationship between the users' concerns for information privacy and users' benefit beliefs.

H1: Users' privacy concern on using LBS has negative influence on users' perceived benefit of using LBS.

Numerous empirical studies showed that information privacy concerns have a significant influence on the perceptions of the level of risk when users exchange their personal information for a web-site membership on Internet[15,20]. Hoffman et al.[6] also found that over 72% of the Internet users were not tend to reveal their personal information because of privacy risk. Second hypothesis is about the relationship between the users' concern for information privacy and users' risk beliefs.

H2: Users' privacy concerns on using LBS has positive influence on users' perceived risk.

Huffman et al.[6]'s analysis revealed that the primary concerns to consumers providing demographic data are related to trust beliefs and the characteristic of the exchange relationship. Trust beliefs can positively influence willingness to disclose privacy information[17]. Users who build trust experience increase of switching costs, which implies continuing the relationship with the firm and bearing the risk of disclosing privacy information[20]. Pavlou and Gefen[21] also argued that there is a "direct positive relationship between a set of trust beliefs about a seller's reliability, honesty, and trustworthiness, and transaction intentions in using an auction website." Next hypothesis examines the relationship between the perceived benefits of LBS users and their intention to use LBS.

H3: Users' perceived benefit of using LBS has positive influence on users' intention to use LBS.

In the context of traditional commercial transactions, consumers are afraid of risks involved in the transactions such as the possibility of being incomplete transactions, unsatisfied quality of goods and services, etc. Online transactions increase the risk even more due to the fact that transactions are performed in the virtual space, and personal and financial information is transmitted over computer network. Moreover the information transmitted to merchants is kepted on the information systems which is owned and operated by merchants. Consumers are afraid of privacy of their information and express concerns about what kind of measures are taken to secure the systems[17].

Because of its intrinsic nature of online transaction, using e-commerce needs the detail information about customers such as name, address and payment information. E-commerce consumers confront with the possibility of privacy risks related to the collection, protection, and use of information[22]. We proposed the forth hypothesis which is about the relationship between Internet users' risk beliefs and their behavioral intention that submit personal information to websites.

H4: Users' perceived risk of using LBS has negative influence on users' intention to use LBS.

4. Data Analysis and Discussion

The data used in this research were collected from undergraduate students who have experience of using LBS during October 2016. A total of 250 questionnaires were distributed to the undergraduate students who have experiences of using LBS, and 220 were returned. Among them 13 were excluded due to missing data or untrustworthy responses (e.g., marking same scale on all questionnaire items). Therefore, 203 questionnaires were used for data analysis. The research model was examined with SmartPLS 2.0.

<Table 2> Convergent Validity and Reliability of First-order Construct

Construct	Item	Loading	t-value	AVE	CR
Collection	Co1	0.632	8.045	0.569	0.838
	Co2	0.659	7.701		
	Co3	0.839	24.469		
	Co4	0.859	26.960		
Errors	Err1	0.813	23.049	0.591	0.852
	Err2	0.721	11.139		
	Err3	0.809	18.905		
	Err4	0.728	12.753		
Secondary Use	SU1	0.875	39.938	0.755	0.925
	SU2	0.882	39.974		
	SU3	0.898	57.174		
	SU4	0.820	24.711		
Improper Access	IA1	0.813	21.114	0.676	0.893
	IA2	0.819	23.614		
	IA3	0.832	28.379		
	IA4	0.823	22.311		
Benefit	Bn1	0.675	11.307	0.550	0.829
	Bn2	0.792	23.942		
	Bn3	0.808	22.050		
	Bn4	0.680	8.361		
Risk	Ri1	0.680	12.746	0.660	0.885
	Ri2	0.850	28.609		
	Ri3	0.859	39.156		
	Ri4	0.848	30.956		
Usage Intention	BI1	0.801	18.132	0.646	0.879
	BI2	0.839	31.105		
	BI3	0.835	24.648		
	BI4	0.736	12.572		

Data analysis began with instrument validation. <Table 2> shows the convergent validity and reliability of constructs used in the research model. Reliability of measurement items is assessed with several statistical methods. First, Cronbach's α measures internal consistency of measurement items and threshold value is above 0.7. Composite reliability (CR) measures common variance among measurement items which consist of same construct. Average variance extracted (AVE) is the variance explained by measurement items in the same construct. Cut-off value for CR is above 0.7 and that of AVE is above 0.5[23]. All measurement items satisfied above mentioned criteria. Therefore, it can be said that they are reliable measures.

Validity is another important aspect of instrument validation process. Two types of validity are commonly mentioned; convergent validity and discriminant validity. Convergent validity means the degree to which all measurement items in the same construct are consistent. If all measurement items are significantly loaded on the respected construct and loading values are exceeding 0.5, they exhibit convergent validity. For the data used in this study, all item loadings were significant at p-value of 0.01. Also all standardized loadings were above 0.5. Hence, all measurement items satisfied the criteria for convergent validity.

<Table 3> Discriminant Validity of Construct

`	Co	Err	SU	IA	Bn	Ri	BI
√AVE	0.75	0.76	0.86	0.82	0.74	0.81	0.80
Co	1.00						
Err	0.44	1.00					
SU	0.54	0.43	1.00				
IA	0.28	0.42	0.44	1.00			
Bn	0.05	0.21	-0.03	0.11	1.00		
Ri	0.35	0.31	0.48	0.37	0.19	1.00	
BI	0.18	0.15	0.15	0.18	0.38	0.18	1.00

Chin[24] explains how to assess discriminant validity. If the square root of AVE for a construct is greater than correlation with other construct, it can be said that those two constructs have discriminant validity. Also, all values of square root of AVE should be greater than 0.7. <Table 3> shows that the measurement items used in this study satisfied the conditions for discriminant validity.

With validated measurement items, research model was assessed to test overall explanatory power. <Table 4> shows R^2 of each endogenous construct and overall explanatory level. If R^2 of an endogenous construct is higher than 0.26, goodness of fit for the construct is high. If it is between 0.13 and 0.26, goodness of fit is average. If it is below 0.13, then goodness of fit is low[25].

Overall explanatory power is assessed by the value of square root of average R^2 value of endogenous constructs multiplied by average of communalities. If it is greater than 0.36, overall fit is high. If it is between 0.25 and 0.36, overall fit is average. If it is below 0.25, the fit is low. <Table 4> indicates that even though fit values for individual construct are rather low, the overall explanatory power index is on average level.

<Table 4> Overall Explanatory Power of Model

Construct	R^2	Redundancy	Communality
Privacy Concerns	-	-	0.540
Benefit	0.003	0.001	0.552
Risk	0.272	0.177	0.661
Usage Intention	0.157	0.092	0.646
Average	0.144	0.09	0.560
Overall Explanatory Level	√(0.144×0.560)=0.294		

<Table 5> shows results of hypothesis test. While H1 and H4 were not accepted, H2 and H3 were accepted at α=0.01 level. Users of LBS concern the exposure of their location information and it affects the perceived level of risk. However, when they decide whether to use LBS, they only consider the benefit provided by LBS. The results are very interesting. It indicates that there is system 1 and system 2 phenomenon described by behavioral economics[26].

<Table 5> Hypothesis Testing

Hypothesis	Path Coefficient	t-value
H1: Privacy Concern → Benefit	0.053	0.441
H2: Privacy Concern → Risk	0.522	8.961
H3: Benefit → Usage Intention	0.360	6.003
H4: Risk → Usage Intention	0.111	1.417

5. Conclusions

With wide use of smartphones, LBS becomes one of the essential services used by smartphones. At the same time, smartphone users are more concern about the information privacy. LBS are not the exception. Users have to provide location information which is essential to use of LBS.

This study focuses on how smartphone users perceive providing location imformation to use LBS. The research model proposed in this study is based on on privacy calculus perspective in which both benefits of using LBS and risks of providing location privacy information are considered.

The research model was empirically validated with data collected from 203 undergraduate students who have experiences of using LBS. Validity and reliability of measurement items were confirmed with extensive instrument validation process. PLS analysis of the model showed that users' privacy concern affects users' perceived level of risk positively while it does not affect perceived benefit of using LBS. On the other hand, users' perceived risk does not affect users' intention to provide privacy information while the perceived benefit does positively affect users' intention.

The findings of this study are very interesting. Users' emotional judgment affects negative side of calculus, but users' behavioral judgment is affected by positive side of calculus. The findings are consistent with system 1 and system 2 theory described in behavioral economics. Privacy paradox phenomenon can also be explained by the results of this study. Future research will be focused on privacy paradox from behavioral economics perspective. It is inevitable to examine user's actual behavior in order to incorporate behavioral aspect of privacy. Further study needs to carry out experimental study to understand actual behavior.

ACKNOWLEDGMENTS

This study was supported by the Fund for Humanities & Social Studies at Pusan National University 2016.

REFERENCES

[1] Hruska, J., "Smartphone usage surges while PCs show startling decline in new worldwide study," Extreme Tech, August 2014.

[2] Zichuhr, K., "Location-Based Services," Pew Research Center, 2013.

[3] Boyles, J., Smith, A, and Madden, M., "Privacy and Data Management on Mobile Devices," Pew Research Center, 2012.

[4] Money Today, "Apple fined 3M won for illegally gathered location information," 2011.

[5] EPIC Alert, "Washington D. C.: Electronic Privacy Information Center," 2000.

[6] Hoffman, D. and T. Novak, "Marketing in Hypermedia Computer-Mediated Environments: Conceptual Foundations," Journal of Marketing, Vol. 60, pp. 50-68, 1996.

[7] Junglas, I. and Watson, R., "Location-based Services: Evaluating user perceptions of location-tracking and location-awareness services," Communications of the ACM, Vol. 51 No. 3, pp. 65-69, 2008.

[8] Jourard, S., "Some Psychological Aspects of Privacy," Law and Contemporary Problems, Vol. 31, pp. 307-318, 1966.

[9] Stone, E., D. Gardner, H. Gueutal, and S. McClure, "A Field Experiment Comparison Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations," Journal of Applied Psychology, Vol. 68, No. 3, pp. 459-468, 1983.

[10] Stone, E. F., and D. L. Stone, "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," in Research Findings in Personnel and Human Resources Management, K. Rowland and G. Ferris (Eds.), JAI Press, pp. 349-411, 1990.

[11] Faja, S. and S. Trimi, "Influence of the Web Vendors' Interventions on Privacy-Related Behaviors in E-Commerce," Communications of the AIS, Vol. 17, pp. 593-634, 2006.

[12] Shin, M., "Influences Information Privacy Concerns and Personal Innovation of Smartphone-based Shopping Mall on Usefulness, Ease-of-Use and Satisfaction," Journal of Digital Convergence, Vol. 12, No. 8, pp. 197-209, 2014.

[13] Campbell, A., "Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes about Information Privacy," Journal of Direct Marketing, Vol. 11, pp. 44-57, 1997.

[14] Smith, H. J., S. J. Milberg and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," MIS Quarterly, Vol. 20, No. 2, pp. 167-195, 1996.

[15] Malhotra, N. K., S. S. Kim and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Casual Model," Information Systems Research, Vol. 15, No. 4, pp. 336-355, 2004.

[16] Cheung, A., "Location privacy: The challenges of mobile service devices," Computer Law & Security Review, Vol. 30, No. 1, pp. 41-54, 2014.

[17] Dinev, T. and Hart, P., "An extended privacy calculus model for e-commerce transactions." Information Systems Research, Vol. 17, No. 1, pp. 61-80. 2006.

[18] Stewart, A. and A. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument," Information Systems Research, Vol. 13, No. 1, pp. 36-49, 2002.

[19] Ajzen, I., "The theory of planned behavior. Organizational behavior and human decision processes," Vol. 50, No. 2, pp. 179-211, 1991.

[20] Mayer, R. C., J. H. Davis, and F. D. Schoorman, "An Integrative Model of Organizational Trust," Academy of Management Review, Vol. 20, No. 3, pp. 709-734, 1995.

[20] Min, H. and G. Hwang, "The effect of Privacy Factors on the Provision Intention of Individual Information from the SNS Users," Journal of Digital Convergence, Vol. 14, No. 12, pp. 1-12, 2016.

[21] Pavlou, P. A. and D. Gefen, "Building Effective Online Market-Places with Institution-Based Trust," Information Systems Research. Vol. 15, No. 1, pp. 37-59, 2004.

[22] Park, C. and J. Kim, "An Empirical Research on Information Privacy Concern in the IoT," Journal of Digital Convergence, Vol. 14, No. 2, pp. 65-72, 2016.

[23] Nunnally, J. C. and Bernstein, I. H., "Psychometric Theory," (3rd Ed.), McGraw-Hill, New York, 1994.

[24] Chin, W. W., "The Partial Least Squares Approach to Structural Equation modelling," Modern methods for business research, Vol. 295, pp. 295-336, 1998.

[25] Cohen, J. O., "Statistical Power Analysis for the Behavioral Sciences," (2nd Ed.), Lawrence Erlbaum: Hillsdale, New Jersey, 1988.

[26] Kahneman, D., "Thinking Fast and Slow," 2011.

김 종 기(Kim, Jong Ki)

- 1992년 12월 : 미국 미시시피주립대 (경영학박사)
- 1999년 3월 ~ 현재 : 부산대학교 경영학과 교수
- 관심분야 : 정보보안, 정보 프라이버시, 기술혁신
- E-Mail : jkkim1@pusan.ac.kr