

인터넷 사용자의 개인정보보호 행동의 차이에 관한 연구

장 초* · 만리리* · 민대환** · 임성택***

Differences in Privacy-Protective Behaviors by Internet Users in Korea and China

Chao Zhang* · Lili Wan* · Daihwan Min** · Seongtaek Rim***

■ Abstract ■

Privacy-protective behavior can be classified into passive behavior and active behavior. Passive behavior includes refusal, misrepresentation, and removal, while word-of-mouth, complaint, and seeking for help belong to active behavior. Internet users in different countries may take different types of privacy-protective behavior because of cultural and social differences. This study analyzes the differences in Internet users' privacy-protective behavior between Korea and China. Korean Internet users take refusal, complaint, and seeking to protect their privacy information, while misrepresentation is not an option for Korean Internet users. Chinese Internet users take refusal, complaint, seeking, and misrepresentation to protect their privacy information. In Korea, passive behavior (refusal) is chosen more often than active behavior (complaint and seeking for help), while in China active behavior (complaint and seeking for help) is preferred to passive behavior (refusal and misrepresentation). The differences of privacy-protective behavior in the two countries may provide some implications for online companies, if they want to avoid the business risk due to privacy concerns and to take appropriate steps to deal with privacy-protective behavior by Internet users.

Keyword : Online Privacy, Privacy Concern, Privacy-Protective Bbehavior, Comparison
Between Korea and China

1. Introduction

A lot of new artifacts come into our daily life, such as social network service, ubiquitous computing, cloud computing, etc. While the new artifacts bring benefits to users, they also generate numerous privacy concerns. According to a poll, 94% of American consumers consider online privacy important [32]. Statistics Canada [31] reported that 74% were concerned or very concerned about online privacy.

Governments, organizations, and individuals have tried to establish ways to protect online information privacy [1-3]. Especially, Internet users will possibly take different types of privacy-protective behavior when they feel their privacy information is threatened. Almost 95% of the Internet users surveyed have declined to provide personal information to online companies at one time or another, which means that many customers may not really trust an online company when making purchases online [14]. IS researchers have focused on privacy concern and other facts related to privacy concern. Culture is found to affect privacy concern in several cross-cultural studies [5, 21, 22]. Although some researchers have suggested several privacy-protective behaviors, culture difference is not considered when studying privacy-protective behaviors.

The objective of this paper is to focus on Internet users' privacy-protective behavior, when they feel online companies threaten their information privacy. This study integrates existing research about privacy-protective behavior and rebuilds the privacy-protective behavior model. Then, this study compares the difference between Korea and China, and tries to explain the

difference by cultural values.

The remainder of this paper is organized as follows: the next section reviews the existing literature; the third section presents the research model; the following section describes how the research is conducted; the fifth section presents results; the discussion section follows, and the final section concludes with implications, limitations, and directions for further research.

2. Literature Review

2.1 Privacy Concern

Internet users' personal information is now a commodity which is routinely bought, sold, and traded. Online companies collect detailed customer information to analyze Internet users' behavior, and to increase the efficiency and effectiveness of their marketing strategies. Actually, it is now impossible for Internet users to transact a business online without having to reveal personal information. Such information could be obtained voluntarily (when consumers provide information during online transactions or while registering to use certain websites) or involuntarily (by use of cookies that track consumers' online surfing behavior) from the part of Internet users.

Information privacy concerns refer to the extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information [29]. It is not only the concern about the information disclosure, but also the degree of control that Internet users have over the collection of information and its subsequent use by online companies. Because of a variety of factors such as

culture, regulatory laws, past experiences, and personal characteristics, Internet users exhibit different levels of concerns about information privacy [20]. Internet users' privacy concerns have received considerable attention as one of the salient factors that determine their willingness or unwillingness to disclose personal information to online companies [10, 20, 29].

2.2 Privacy-Protective Behaviors

Internet users who are concerned about their online information privacy would be cautious in most of their Internet-based activities. They might think that online companies may misuse their personal information and lead to considerable loss [10, 33]. Thus, Internet users will take some kinds of privacy-protective behavior, such as complaint or negative word-of-mouth [23], supplying false or fictitious information to a website [18], managing the use of cookies [9], and even refusing to purchase from particular websites [8] to prevent such opportunism and minimize the loss from misuse. Some researchers identified three kinds of customer behavior: exit the relationship with sellers, voice their dissatisfaction to the seller, and show loyalty to the seller by neither exiting nor voicing [13, 27, 28]. Singh [28] also expanded the taxonomy to three categories: voice (complaints directed at the seller or manufacturer), private (informal complaints involving friends and relatives such as negative word of mouth), and third party responses (formal complaints directed toward public agencies not directly involved in the exchange). Cho et al. [7] classified privacy-protection behaviour into three types: the avoidance type consists of items such as 'use of non-

Internet means to communicate, buy, or gather information'. The opt-out type has to do with actively choosing not to receive email solicitations. The proactive protection type addresses more active protection of personal information, such as using privacy enhancing technologies, erasing cookies, checking trust marks, etc. Son and Kim [30] classified privacy-protective behavior into information provision action (refusal and misrepresentation), private action (removal and negative word of mouth), and public action (complaining directly to online companies and complaining indirectly to third-party organizations). Park [24] classified information control behavior into social dimension and tech dimension. Within the social dimension, distinction between active and passive control was made.

From the previous research, this study identifies privacy-protective behavior by Internet users' and classifies them into six different kinds: refusal, misrepresentation, removal, word-of-mouth, complaint, and seeking. These six kinds of privacy-protective behavior can be grouped into two types, active and passive. Active behavior contains word-of-mouth, complaint, and seeking, while passive behavior includes refusal, misrepresentation, and removal (See <Table 1> and <Table 2>).

3. Research Model and Hypotheses

3.1 Research Model

A research model was developed to investigate the impact of privacy concern on privacy-protective behaviors [Figure 1].

Refusal may take place in various situations.

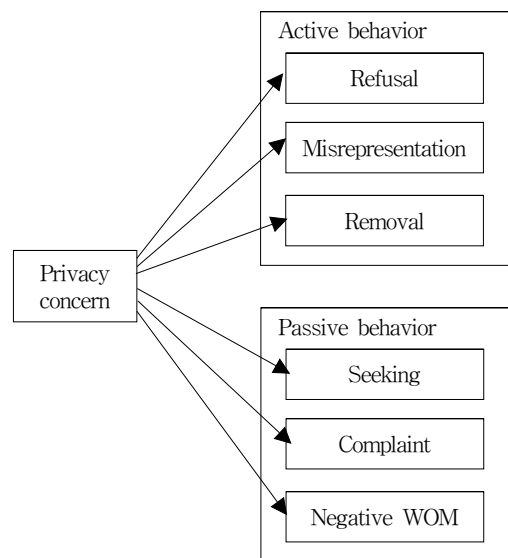
<Table 1> Active privacy-protective behaviors

Behavior	Definition	Source
Refusal	"Refusal" refers to Internet users' refusal to provide their personal information to online companies.	[19, 30]
	"Refrain" represents users' refusal to use the web site that asks them to provide personal information.	[34]
	"Refusal" to e-Commerce means unwillingness to provide personal information and use the website.	[4]
	"Refusal" means Internet users refuse to purchase and visit online companies' website, or even refuse to register	[17, 19, 24, 25, 34]
Misrepresentation	"Misrepresentation" means to falsify the personal information or incorrect personal information submitted to online companies.	[19, 24, 25, 30, 34]
	"Fabricate" refers to young adolescents' efforts to falsify their information or provide incomplete information.	[19, 25, 34]
Removal	"Removal" means deleting his or her personal information from online companies' databases.	[24, 29, 30]
	"Removal" means to request removal from mailing lists.	[25]

Internet users would refuse to provide personal information to online companies, refuse to purchase from those online companies' websites, and even refuse to use such websites [4, 17, 19, 25, 30, 34]. Internet users without privacy concerns will show three behaviors : willingness to provide personal information, acceptance of e-commerce, and willingness to use Internet [4]. Internet users with privacy concern may refuse to provide personal information in response to a request from online companies [10]. Internet users' "refusal" includes refusal to register for a membership of a website, refusal to purchase from an online company's website, and even refusal to

<Table 2> Passive Privacy-Protective Behaviors

Behavior	Definition	Source
Word-of-Mouth	"Negative word-of-mouth" refers that Internet users may share their negative experiences with their friends and relatives when online companies threaten their information privacy.	[30]
	Internet users with no privacy concern will recommend online companies' website to others.	[17]
	Negative remark or comments about a website	[17]
	"Complaint" means to contact the company or independent third-party privacy-protection groups for complaining.	[24, 30]
Complaint	"Flaming" means to send highly negative messages.	[25]
	Internet users may notify Internet service providers about unsolicited e-mail.	[25]
Seeking	"Seek" refers to one's efforts to ask others for advice or to read the privacy statement.	[34]
	Use of privacy enhancing technologies	[19, 24]



[Figure 1] Research Model

use. Internet users' refusal to provide their personal information to online companies is believed to be an important form of information protective behavior. Thus, we hypothesize :

H1 : If privacy concern is higher, Internet users' refusal to register, to purchase, and to use a website of online companies would be stronger.

Misrepresentation describes the following behaviors : Internet users will provide incorrect or incomplete personal information to online companies which may threaten their privacy [19, 25, 30, 34]. Misrepresentation is a "guerilla tactic" used by individuals in order to defend their privacy. Over 30% of Internet users admitted to routinely giving false or fictitious information to websites [8], while more than half (51%) reported that they falsified or misrepresented data at least occasionally [11]. Obviously, Internet users' falsification of their personal information to online companies will be a less costly and more convenient choice. The next hypothesis is :

H2 : If privacy concern is higher, Internet users' misrepresentation to give incorrect and incomplete information to online companies would be stronger.

Removal can be considered as a privacy-protective behavior that Internet users will remove their personal information from online companies' database or mailing lists when they feel privacy threatened. Internet users' "removal" is a specific action that can be taken in response to an information privacy threat by removal of their personal information from online companies' da-

tabases [29, 30]. This leads to the following hypothesis :

H3 : If privacy concern is higher, Internet users' removal of personal information from the databases of online companies would be stronger.

Internet users' "word-of-mouth" means they may share their experiences with other people about the online company, recommend a website to others, and give remarks or comments about a website. There are two different kinds of word-of-mouth, positive or negative word-of-mouth. In this paper, if Internet users feel privacy threatened by online companies, they may give "negative word-of-mouth", which means to share their negative experiences with others, not to recommend online companies' website to others, and to give negative remarks about online companies [17]. This suggests :

H4 : If privacy concern is higher, Internet users' negative word-of-mouth about online companies' threats to their personal information would be stronger.

Complaint can be used to describe a kind of privacy-protective behavior that directly or indirectly complain to various organizations. When Internet users are dissatisfied with handling of their personal information, they may take three kinds of complaining behavior to minimize their loss. They complain directly to online companies by calling or sending e-mail, complain indirectly to third-party organizations such as consumer protection office, and notify Internet Service Provider (ISP) about unsolicited e-mail [25, 30]. The

primary goal of taking public action is to seek a specific remedy [26]. Dissatisfied customers generally take action through third-party organizations when they do not obtain satisfactory redress by direct complaints [27]. Thus, we propose :

H5 : If privacy concern is higher, Internet users' complaining about online companies' threats to their personal information would be stronger.

“Seeking” refers to Internet users’ efforts to ask others for advice, read the privacy statement, or use some privacy enhancing technologies and tools to safeguard their online privacy, such as anonymizers, encryption technologies, Pretty Good Privacy (PGP), anti-spam filters, re-mailers, e-mail shredders, cookie-busters, and HTML filters [19, 34]. One in 20 users had employed software to hide their computer’s identity from websites [11], while one in four had set their browsers to reject cookies [8]. This suggests the last hypothesis :

H6 : If privacy concern is higher, Internet users' seeking for advice of other people, reading the privacy statement, or using privacy enhancing technologies would be stronger.

4. Research Method

This section describes the scale development, the sample, and data collection process.

4.1 Scale Development

Most of the measurement scales for research constructs in this study were adapted from ear-

lier studies in which the measurement scales were proven to be reliable and valid. This study measured the privacy concern with four dimensions : collection (COLL), errors (ER), unauthorized secondary use (US), and improper access (IA), using multiple items on seven-point Likert scales. And also, this study measured the six specific kinds of privacy-protective behaviors :

〈Table 3〉 Scale Development

Construct	Dimension	Source
Refusal	Refusal to register	[19, 30, 34]
	Refusal to purchase	
	Refusal to use	
Misrepresentation	Giving incorrect personal information	[19, 30, 34]
	Giving incomplete personal information	
Removal	Removing personal information from online companies' database	[25, 30]
Word-of-Mouth	Sharing negative experiences with others to offend online companies	[17, 30]
	Recommendation of a website to others	
	Negative remark or comments about a website	
Complaint	Complaint directly to online companies	[25, 30]
	Complaint indirectly to third-party organization	
	Notifying ISP about unsolicited e-mail	
Seeking	Asking others for advice	[19, 34]
	Reading privacy statement	
	Using privacy enhancing technologies	
Privacy Concern	Collection	[20, 29]
	Errors	
	Unauthorized secondary use	
	Improper access	

refusal, misrepresentation, removal, word-of-mouth, complaint, and seeking, using multiple items on seven-point Likert scales (Refer to <Table 3>).

The survey questionnaires were translated into Korean and Chinese. Nine Korean student and seven Chinese students were asked to do a pilot test. After the pilot study, minor changes to some questions were made. The order of this study's survey questionnaires was randomized so that more reliable data could be collected.

4.2 Data Collection

The purpose of this research is to analyze different kinds of the Internet users' privacy-protective behavior in Korea and China. So the Internet users were the target population for data collection. The final survey was administered to college students in China and Korea. After deleting the responses with missing and inconsistent data, 250 Korean data and 246 Chinese data were used for the data analysis. All the Korean respondents were undergraduate students and Chinese respondents include undergraduate students, company employees, and MBA students. Among all of the Chinese respondents, 99.6% were students; 79.3% were between 21~25 years old; and 52.4% were female. They also reported that 67.8% of them spent about 1~3 hours a day on average on the Internet and 46.3% had used the Internet for more than 5 years. Among all of the Korean respondents, 99.6% were students; 71.7% were between 21~25 years old; and 49.6% were female. They also reported that 67.6% of them spent about 1~3 hours a day on average on the Internet and 96.7% had used the Internet for more than 5 years.

5. Data analysis and Results

5.1 EFA(Exploratory Factor Analysis)

First of all, this study used exploratory factor analysis in order to examine the relationships among variables and to determine whether data can be condensed or summarized into a smaller set of factors. Varimax for factor rotation was used.

<Table 4> Result from EFA and Reliability

Constructs	Items	Factor loading	Cronbach's alpha
Privacy concern	PC5	0.821	0.891
	PC7	0.815	
	PC9	0.807	
	PC10	0.793	
	PC6	0.753	
	PC2	0.691	
	PC8	0.649	
	PC1	0.615	
Refusal	RF2	0.801	0.776
	RF3	0.736	
	RF1	0.703	
	RF6	0.699	
	RF4	0.610	
Complaint	COMP1	0.866	0.790
	COMP3	0.817	
	COMP2	0.663	
	COMP4	-0.582	
Seeking	S5	0.796	0.797
	S3	0.764	
	S4	0.717	
Misrepresentation	M2	0.883	0.818
	M1	0.827	

As shown in <Table 4>, all items were fallen into five factors : privacy concern, refusal, com-

plaint, seeking, and misrepresentation. After the exploratory factor analysis, two constructs of removal and negative word-of-mouth were deleted, since the items of removal were not separated from refusal and the items of negative word-of-mouth belonged to other behavioral factors.

Removal refers to the action of deleting personal information from online companies' database, which can be thought as one kind of refusal behavior to some extent. Although negative word-of-mouth was recognized as a privacy-protective behavior in some existing literature with American data, it is not true for Asian data in this research. Negative word-of-mouth is not viewed as a clear concept that is different from other privacy-protective behavior by Korean and Chinese Internet users. There exist a few studies that combined negative word-of-mouth and complaint as one factor [27, 28]. The reliability analysis showed that the Cronbach's alpha values of all factors were over 0.7, which meant these factors have good reliability.

5.2 Structural Equations Modeling

The structural equation modeling was used. It is particularly useful in testing the research model that contains multiple equations involving dependence relationships.

5.2.1 Confirmatory Factor Analysis

Confirmatory factor analysis (CFA) was used to assess the measurement quality of constructs. CFA can test or confirm a specified relationship. Each item can only load on its prespecified factor while the factors themselves were allowed to correlate freely. Various overall fit indices indicated a reasonable fit of the model to the data,

and all the goodness of fit indices for confirmatory factor analysis is beyond the acceptable level.

<Table 5> Fitness Indices of Measurement Model

Indices	χ^2	$\chi^2/df(46)$	RMSEA	GFI	AGFI
Result	95.673	2.080	0.047	0.968	0.946
Indices	SRMR	CFI	NFI	TLI	IFI
Result	0.029	0.982	0.966	0.974	0.982

The fit indices of the measurement model ($\chi^2(46) = 95.673$) for the overall data are as follows : $\chi^2/DF = 2.080$, root mean square error of approximation [RMSEA] = 0.047, standard root mean square residual [SRMR] = 0.029, comparative fit index [CFI] = 0.982, normed fit index [NFI] = 0.966, goodness-of-fit index [GFI] = 0.968, adjusted goodness-of-fit index [AGFI] = 0.946, Tucker-Lewis Index [TLI] = 0.974, and incremental fit index [IFI] = 0.982.

5.2.2 Convergent and Discriminant Validity

Convergent validity is the degree to which a manifest variable is similar to other variables that measure the same construct, while operationalization is not similar to (diverges from) other operationalizations [6].

<Table 6> AVE and Square of Correlation Coefficients

	RF	COMP	S	PC	M
RF(Refusal)	0.810				
COMP(Complaint)	0.009	0.551			
S(Seeking)	0.002	0.196	0.505		
PC(Privacy Concern)	0.143	0.116	0.038	0.525	
M(Misrepresentation)	0.004	0.029	0.219	0.003	0.826

Note) Diagonal cells show AVE values.

As shown in on diagonal cells of Table 6, all the average variance extracted (AVE) values of the overall data are higher than 0.5, which means the items in this study have convergent validity. All the squares of correlation coefficients between factors are lower than AVE, which also means the items in this study have discriminant validity.

5.2.3 SEM Analysis

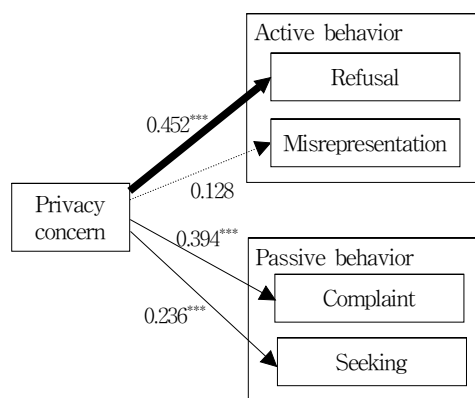
The SEM analysis was followed to determine the strength of the paths shown in the revised research model where ‘removal’ and ‘word of mouth’ were deleted from the original research model. The goodness-of-fit indices for the overall data ($\chi^2(105) = 219.354$) are as follows : $\chi^2/DF = 2.089$, root mean square error of approximation [RMSEA] = 0.047, standard root mean square residual [SRMR] = 0.077, comparative fit index [CFI] = 0.957, normed fit index [NFI] = 0.921, goodness-of-fit index [GFI] = 0.933, adjusted goodness-of-fit index [AGFI] = 0.900, Tucker-Lewis Index [TLI] = 0.946, and incremental fit index [IFI] = 0.957.

<Table 7> Fitness Indices of Structural Model

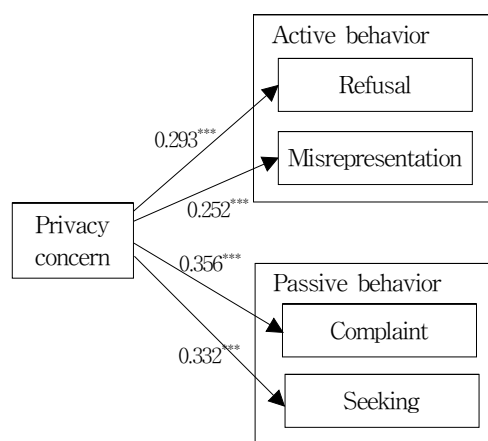
Indices	χ^2	$\chi^2/df(105)$	RMSEA	GFI	AGFI
Result	219.35	2.089	0.047	0.933	0.900
Indices	SRMR	CFI	NFI	TLI	IFI
Result	0.077	0.957	0.921	0.946	0.957

The results from two separate SEM analyses are shown in <Table 8>, [Figure 2], and [Figure 3] for Korean and Chinese data. The Korean data supported that privacy concern significantly affected three types of privacy-protection behavior such as refusal, complaint, and seeking. But the effect of privacy concern on misrepresenten-

tation is not significant. The standard regression weight between privacy concern and refusal was the highest (0.452) among the three significant relationships. Refusal as a passive kind of privacy-protective behavior was much stronger than active kinds of privacy-protective behavior such as complaint and seeking.



[Figure 2] Results of Korean Data



[Figure 3] Results of Chinese Data

In contrast, the Chinese data supported all four dependence relationships from privacy concern to refusal, complaint, seeking, and misrepresentation.

〈Table 8〉 Results of hypotheses test

H	Relationship	Korea			China		
		Standard regression weight	P value	Result	Standard regression weight	P value	Result
H1	Privacy concern → refusal	0.452	0.000	Support	0.293	0.000	Support
H2	Privacy concern → misrepresentation	0.128	0.61	No support	0.252	0.000	Support
H5	Privacy concern → complaint	0.394	0.000	support	0.356	0.000	Support
H6	Privacy concern → seeking	0.236	0.000	support	0.332	0.000	Support

The standard regression weights between privacy concern and four types of privacy-protective behavior were not much different, although active privacy-protective behavior (complaint and seeking) is a little stronger than passive privacy-protective behavior (refusal and misrepresentation).

The statistical difference between the two countries was also tested using between-group analysis of AMOS. For the free model, all the path coefficients are set free.

In the constrained model, each of the path coefficients of two countries was set to be the same respectively, and then compare the increase in χ^2 . As the degree of freedom increased by 1, the increases of χ^2 were all less than 3.84, so the hypothesis that the path coefficients are the same for two countries can't be rejected, which means there are no difference in the relationship of privacy concern and privacy-protective behavior between Korea and China.

6. Discussion

The relationship between privacy concern and misrepresentation is significant with Chinese data but not significant with Korean data. South Korea has implemented a comprehensive Internet real-name policy regulating users of emails, on-

line forums, blogs, online videos, and many other Internet services. For those who want to apply for an email or online chatting service account in South Korea, they have to fill out a form first, providing detailed information including their real name, address, identity number, and profession. In Korea, it is hard to input incomplete and spurious personal information because of Internet real name policy. Identification number and name are checked with the official database. If they fail to match, the registration is refused. The similar situation happens when a cell phone number is input. The applicants have to input the security code they get from their mobile phone to prove that they are the owner of the phone number. As a result, there is nearly zero possibility to take a misrepresentation behavior. There is no such Internet real name policy in China, so the misrepresentation is a possible choice for Chinese Internet users as privacy-protective behavior. The same result happened in the existing literature with American data. However, the relationship between privacy concern and misrepresentation was not significant in the US [30].

With Korean data, the results show that the relationship between privacy concern and passive privacy-protective behavior (refusal) is higher than the relationship between privacy con-

cern and active privacy-protective behavior (complaint and seeking). But with Chinese data, the results show that the relationship between privacy concern and active privacy-protective behavior (complaint and seeking) is higher than the relationship between privacy concern and passive privacy-protective behavior (refusal and misrepresentation). The differences can be explained by the difference in cultural values between China and Korea. China shows stronger masculinity, stronger long-term orientation, and weaker uncertainty avoidance than Korea [15, 16].

First, masculinity/femininity is the extent to which emotional gender roles are recognized with respect to work. Individuals with masculine values emphasize work goals, assertiveness, and achievement. In contrast, feminine values include nurturing, concern for others, and quality of life [15]. People in higher masculinity culture may take active actions of seeking help by using privacy-protective software and complaining when they feel privacy threatened by online companies. People in weaker masculinity culture take more passive actions just to refuse to give personal information.

Second, long-term orientation refers to the extent to which an individual adheres to forward thinking. Individuals with high long-term orientation will be inclined to consider long-term commitments as valuable. Long-term orientation is associated with good buyer-seller relationship [12]. Individuals with higher long-term orientation care about not just one transaction on the website but want to have a good relationship with the website and continue to use the website in the future. Chinese Internet users with higher long-term orientation will use complaint to force the online company to improve their pri-

vacuity-protective service, or use seeking for help to advance their own privacy-protective ability, in order to keep using the website in the future. Korean Internet users with relatively lower long-term orientation care about each transaction and make a decision each time when they visit a website. As a result, refusal is more often used.

Last, uncertainty avoidance deals with a society's tolerance for uncertainty and ambiguity. It indicates the extent to which individuals feel either uncomfortable or comfortable in novel, unknown, uncertain, or ambiguous situations, and try to avoid these situations. Korean Internet users with higher uncertainty avoidance may tend to take refusal to avoid any ambiguity in the website. In contrast, Chinese Internet users with relatively lower uncertainty avoidance may think that they have more control in the situation, so they express more complaints and seek more help.

7. Conclusion

The main objective of this study is to find the differences in Internet users' privacy-protective behavior between Korea and China. This study classifies privacy-protective behavior into six categories, such as refusal, misrepresentation, removal, word-of-mouth, complaint, and seeking. Internet users in different countries may exhibit different types of privacy-protective behavior because of social and cultural differences. The result shows that Korean Internet users take refusal, complaint, and seeking, but not misrepresentation when they have privacy concerns about the website. Chinese Internet users take refusal, complaint, seeking, and misrepresentation. For Korean Internet users, refusal is the

strongest behavior they would take when they have a high privacy concern, while in the Chinese model the possibility to take four kinds of privacy-protective behavior is not much different.

The findings from this study generally indicate that privacy-protective behavior resulting from privacy concerns is often due to more complex social and cultural reasons. Online companies need to address privacy concerns by online consumers that can undermine a firm's marketing effectiveness. The lack of attention to the Internet users' responses is problematic because it is not mere concerns but actual behavior that may have direct impacts on customer-firm relationships and ultimately on a firm's overall performance. Managers of online companies should know firstly about various types of Internet users' privacy-protective behavior. The differences in two countries may suggest implications for online companies to prepare for different kinds of privacy-protective behavior in different countries.

In Korea, managers should take measures to reduce Internet users' refusal by being honest and trustworthy in dealing with personal information and by avoiding unauthorized secondary use. In China, managers should communicate to the complainants clearly and patiently about when, what, and how online companies will take a corrective and efficient action to handle their complaint.

This study has a few limitations which suggest further research. Firstly, although Korea and China have different cultural value, both countries belong to Asian culture. As a result, the differences between Korea and China are not statistically significant. Further cross-cultural re-

search on privacy-protective behavior should be conducted between western culture and eastern culture.

Secondly, the sample is mainly college students, which may make the generalizability of this study very limited. Future research with more diverse samples is needed.

Finally, two types of privacy-protective behavior (removal and word-of-mouth) were not included in the final research model. More refined questions for the deleted factors and more responses may be necessary.

References

- [1] 김범수, "개인정보관리자의 책임과 벌칙의 형평성", 『한국IT서비스학회지』, 제10권, 제4호(2011), pp.21-32.
- [2] 안연식, "정보보호 안전진단 대상자 선정 기준의 개선 방안 연구", 『한국IT서비스학회지』, 제8권, 제1호(2009), pp.47-58.
- [3] 유기훈, 최웅철, 김신곤, 구천열, "학내 정보보호지침 수립에 관한 연구", 『한국IT서비스학회지』, 제7권, 제1호(2008), pp.23-43.
- [4] Bandyopadhyay, S., "Antecedents and consequences of consumers' online privacy concerns", *Journal of Business*, Vol.7, No.3(2009), pp.41-48.
- [5] Bellman, S., E. J. Johnson, S. J. Kobrin, and G. L. Lohse, "International Differences in Information Privacy Concerns : A Global Survey of Consumers", *The Information Society*, Vol.20, No.5(2004), pp.313-324.
- [6] Campbell, D. and D. Fiske, "Convergent and discriminant validation by the multitrait-multimethod matrix", *Psychological Bulletin*, Vol.56, No.2(1959), pp.81-105.
- [7] Cho, H., M. Rivera-Sánchez, and S. S. Lim,

- “A Multinational Study on Online Privacy : Global Concerns and Local Responses”, *New Media Society*, Vol.11(2009), pp.395-416.
- [8] Culnan, M. J. and G. R. Milne, The Culnan-Milne survey on consumers and online privacy notices, 2001, available at : <http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf>, accessed on November 3, 2011.
- [9] Culnan, M. J. and R. J. Bies, “Consumer Privacy : Baancing Economic and Justice Considerations”, *Journal of Social Issues*, Vol. 59, No.2(2003), pp.323-342.
- [10] Dinev, T. and P. Hart, “An Extended Privacy Calculus Model for E-Commerce Transactions”, *Information Systems Research*, Vol. 17, No.1(2006), pp.61-80.
- [11] Fox, S., R. Lee, J. Horrigan, A. Lenhart, S. Tom, and C. Carter, Trust and privacy online : Why Americans want to rewrite the rules, *The Pew Internet and American Life Project Report*, 2000.
- [12] Ganesan, S., “Determinants of Long-Term Orientation in Buyer-Seller Relationships”, *Journal of Marketing*, Vol.58, No.2(1994), pp.1-19.
- [13] Hirschman, A. O., *Exit, Voice and Loyalty : Responses to Decline in Firms, Organizations and States*, Harvard University Press, Cambridge, MA., 1970.
- [14] Hoffman, D. L., T. P. Novak, and M. Peralta, “Building consumer trust online”, *Communications of the ACM*, Vol.42, No.4(1999), pp.80-85.
- [15] Hofstede, G., *Culture’s Consequences : International Differences in Work Related Values*, Beverly Hills, CA : Sage, 1980.
- [16] Hofstede, G., *Cultures and Organizations : Software of the Mind*, New York : McGraw-Hill, 1991.
- [17] Liu, C., J. Marchewka, J. Lu, and C. Yu, “Beyond concern : A privacy trust-behavioral intention model of electronic commerce”, *Information and Management*, Vol.42, No.2(2005), pp.289-304.
- [18] Lwin, M. O. and J. D. Williams, “A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online”, *Marketing Letters*, Vol.14, No.4(2003), pp.257-272.
- [19] Lwin, M. O., J. Wirtz, and J. D. Williams. “Consumer Online Privacy Concerns and Responses : A Power-Responsibility Equilibrium Perspective”, *Journal of the Academy of Marketing Science*, Vol.35, No.4(2007), pp.572-585.
- [20] Malhotra, N., 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.4(2004), pp.336-355.
- [21] Milberg, S. J., S. J. Burke, H. J. Smith, and E. A. Kallman, “Values, Personal Information, Privacy and Regulatory Approaches”, *Communications of the ACM*, Vol.38, No.12 (1995), pp.65-74.
- [22] Milberg, S. J., H. J. Smith, and S. J. Burke, “Information Privacy : Corporate Management and National Regulation”, *Organization Science*, Vol.11, No.1(2000), pp.35-57.
- [23] Milne, G. R., “Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy : A Research Framework and Overview of the Special Issue”, *Journal of Public Policy and Marketing*, Vol.19, No.1(2000),

- pp.1-6.
- [24] Park, Y. J., "Digital Literacy and Privacy Behavior Online", *Communication Research*, published online before print, 2011.
- [25] Sheehan, K. B. and M. G. Hoy, "Flaming, complaining, abstaining : How online users respond to privacy concerns", *Journal of Advertising*, Vol.28, No.3(1999), pp.37-51.
- [26] Singh, J., "Consumer Complaint Intentions and Behavior : Definitional and Taxonomical Issues", *Journal of Marketing*, Vol.52, No.1(1988), pp.93-107.
- [27] Singh, J., "Determinants of Consumers Decisions to Seek Third Party Redress : An Empirical Study of Dissatisfied Patients," *Journal of Consumer Affairs*, Vol.23, No.2 (1989), pp.329-363.
- [28] Singh, J., "A Typology of Consumer Dissatisfaction Response Styles", *Journal of Retailing*, Vol.66, No.1(1990), pp.57-99.
- [29] Smith, H. J., S. J. Milburg, and S. J. Burke, "Information Privacy : Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly*, Vol.20, No.2(1996), pp. 167-196.
- [30] Son, J.-Y. and S. S. Kim, "Internet Users' Information Privacy-protective Responses : A Taxonomy and a Nomological Model", *MIS Quarterly*, Vol.32, No.3(2008), pp.503-529.
- [31] Statistics Canada, Table 358-0128-Canadian Internet use survey, Internet use, by age group and Internet privacy concern, 2010.
- [32] TRUSTe, 2011 Consumer Research Results : Privacy and Online Behavioral Advertising, 2011, <http://www.truste.com/ad-privacy/> accessed Nov. 30, 2011.
- [33] Van Slyke, C., J. T. Shim, R. Johnson, and J. Jiang, "Concern for Information Privacy", *Journal of the Association for Information Systems*, Vol.7, No.6(2006), pp.415-444.
- [34] Youn, S., "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents", *Journal of Consumer Affairs*, Vol.43, No.3 (2009), pp.389-418.

◆ 저 자 소 개 ◆

**Chao Zhang (kberry@korea.ac.kr)**

Chao Zhang is a doctoral student of Digital Management Department in Korea University in Korea. He holds a Bachelor degree from Shandong Economic College, a second Bachelor degree from Beijing University in China, and a master degree from Korea University. His research interests include areas such as e-commerce system, online privacy and online security.

**Lili Wan (wanll@korea.ac.kr)**

She is a doctoral student of Digital Management Department in Korea University in Korea. She holds a Bachelor degree from Tongji Medical College of Huazhong University of Science and Technology and a Master degree from Beijing Union Medical College (Tshinghua University medical college) in China. Her research interests include areas such as medical information system, e-business, online privacy, and mobile business.

**Daihwan Min (mismdh@korea.ac.kr)**

Daihwan Min is a professor of digital management/management information systems at Korea University Sejong Campus in Korea. He has a BBA degree from Seoul National University and a Master degree in industrial engineering from KAIST, and a Ph.D. degree in business administration from the University of Michigan. His research interests include diverse areas such as business process management, online privacy, e-business strategy, systems analysis, service management, and mobile business.

**Seongtaek Rim (misrim@korea.ac.kr)**

Seongtaek Rim is a professor of Management Information Systems at Korea University, Sejong Campus and a director of the Digital Convergence Research Institute. He received his M.A. and Ph. D degrees in Computer Information Systems from Georgia State University. His research interests span the business value of information technology investment; telecommunication business models and strategy; national ICT policies, etc. He is starting a new work of the economic impact of national ICT investments with ETRI (Electronics and Telecommunications Research Institute).