Asia Pacific Journal of Information Systems
Vol. 25 No. 2 (JUNE 2015), 289-305

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
http://dx.doi.org/10.14329/apjis.2015.25.2.289

What Affects the Value of Information Privacy on SNS?

Woo-Jin Jung[a], Sang-Yong Tom Lee[b,*]

[a] *Post-Doctoral, Graduate School of Information, Yonsei University, Korea*
[b] *Professor, School of Business, Hanyang University, Korea*

A B S T R A C T

The dramatic growth of social networking sites (SNS) has created a myriad of privacy concerns. Our study focuses on how much monetary incentive SNS users are willing to accept in exchange for disclosing their SNS information by accepting friend requests. First, we focused on information privacy in SNS, and estimated the value of information privacy by using the contingent valuation method. Second, we attempted to estimate how SNS users' willingness to accept would change when demographic information and additional information vary. Privacy-sensitive SNS users have the following characteristics: higher education, less SNS experience, and higher security consciousness. On the contrary, those who make good use of SNS and use open-based SNS are less sensitive to privacy. In summary, privacy-sensitive SNS users are fearful or uneasy when they have insufficient control of SNS information. Considering 14 conditions on the value of information privacy on SNS, the mean value of SNS information per person is 173,957 won. If we apply this value to Facebook users, the total Facebook information value would be 1.91 trillion won, considering that there are 11 million users in Korea.

Keywords: Social Network Services (SNS), Contingent Valuation Method (CVM), Willingness to Accept (WTA), Information Privacy, Privacy Concern

Ⅰ. Introduction

Social networking service (SNS) has become one of the greatest social technological phenomena of the 21st century, as it allows users to both express their individuality and meet people with similar interests. SNS is designed to form new network and strengthen relationship between friends and colleagues. Especially, SNSs, such as Facebook, KakaoStory, Band and Twitter, have become new methods of communication as a replacement of online chatting, text message and phone calling. However, the reputation of SNS has been tarnished by various incidents in news media.

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2012-2012S1A3A2033291). The online survey of this study was performed by 'Embrian', a research company.

*Corresponding Author. E-mail: tomlee@hanyang.ac.kr Tel: 82222201814

The dramatic growth of SNS has created a myriad of privacy concerns. Privacy concerns are much more noticeable in SNS than other media such as personal websites like blogs. However, SNS users are not fully aware of these privacy concerns. By placing information on SNS, SNS users make themselves vulnerable to online predators who may sell their information to third parties. This problem is intensified owing to the fact that communicating via SNS has become not only popular but also fashionable and necessary to maintain their social status among 'friends' (Wallbridge, 2009).

Most SNSs provide users with a choice of who can view their profile. This is supposed to prevent unauthorized users from accessing their information. By making their profile private, SNS users can select who may see their page, allowing only him or her added as "friends" to view their profile and preventing undesirable viewing of the profile by other users. They are trying to create a structural obstacle between their privacy and friend addition. Nevertheless, privacy on SNS can be undermined by many factors. For example, SNS users may disclose the information about themselves, SNSs may not take adequate steps to protect the information of SNS users, and third parties frequently may use information about SNS users posted on SNS for a variety of purposes (Rosenblum, 2007).

Research on this information privacy concerns typically seeks to explain differences in levels of privacy concern or to explore the effects of privacy concerns on the willingness to provide personal information or the willingness to transact online (Dinev and Hart, 2006; Malhotra et al., 2004; Milberg et al., 2000; Smith et al., 1996; Stewart and Segars, 2002; Van Slyke et al., 2006). According to an advanced research, attributes of SNS user can be classified into three parts (privacy guardians, information sellers, and convenience seekers). The research concluded that SNS users would rather present their information than anxious when the use of certain SNS could be economically rewarded (Hann et al., 2007). According to another, privacy concerns have been found to differ between SNS users according to sex and personality. For example, women are less likely to invade information privacy; openness, extraversio n, and conscientiousness were found to positively affect the willingness to expose data, while neuroticism decreases the willingness to expose information (Schaar et al., 2013).

This information of SNS privacy is suited to a gift economy because it is a non-rival good and may be gifted at no cost (Mackaay, 1990; Heylighen, 2007). Few SNS charge money for membership. This may be because SNS is a relatively new service, and the value of using SNSs has not been established in users' minds. Information privacy is a very current and exciting research domain that will continue to evolve as new technologies and new initiatives further push the limit of access to information (Bélanger and Crossler, 2011)

We conducted a principal study, which examined the information privacy issues on SNS. No one can control the range of information privacy that may be disclosed in many ways, which makes it necessary to estimate the value of information privacy going around SNS. Our study focuses on how much SNS users are willing to accept monetarily for disclosing their SNS information by accepting friend offer. First, we focused on the matter of information privacy caused by SNS and estimate the value of information privacy by using the contingent valuation method (CVM), which is an influential method to evaluate stated preference. Second, we tried to estimate how willingness to accept (WTA) would change when demographic information (including age, gender, ed-

ucation, monthly expenditure, years of experience using SNS, and number of hours or frequency of SNS use each day) as well as the additional information (including user satisfaction, perceived security level, use ability, follower number, and structure of SNS) varies.

This paper would help us figure out the factors that affect the value of information privacy and derive implications for information privacy administration on SNS. We conducted this approach because there have been no literature about how important a user perceives information privacy on SNS and the official market to sell personal information has never been formed. We made the results on the value of information privacy on SNS more persuasive by analyzing an ordinal multinomial regression model.

This review is organized as follows: We begin by discussing literature of SNS and information privacy concerns on SNS. Then, we present our data and methodology, including a description of the CVM and WTA. Having done that, we discuss the results of our empirical findings. Finally, based on our results, we suggest a new focus for the future research.

Ⅱ. SNS and Information Privacy

SNS is a 'platform' to build social networks among people who share interests, activities, backgrounds or real-life connections. Then, it is 'web-based services' that allow an SNS user to create a public profile, to create a list of SNS users with whom to share associations, and view and cross the associations within the system. It is also considered as 'online community service' though in a broader sense. It allows users to share ideas, pictures, posts, activities, events, interests with people in their network. People use SNS in finding old friends, meeting new friends, or locating people who have the same interests or problems. The most basic of them are visible profiles with a list of "friends" (Boyd and Ellison, 2007). SNS makes it easy to upload many different forms of information privacy, such as age, contact information (including home address and telephone numbers), photos, sexual orientation, and music preferences. People spend an unprecedented amount of time interacting with SNS and uploading large quantities of personal information (Lohr, 2010). There are even different forms where information on SNS are accessed, and updated without the user's permission (Boyd, 2007). Also, there is an issue that the information on SNS may be retained and passed to third parties. With this enormous amount of information on SNS, there are many commercial opportunities for businesses on SNS. Marketers who target a specific kind of consumers can use information gathered from SNS for purposes other than what users intend.

Information on SNS is about information privacy on basic profile, location, interests, political inclination, acquaintances, businesses and smart-phone use. When editing information on a certain SNS account to protect user's information privacy, SNS requires you to login or provide a password. This is designed to prevent unauthorized SNS users from adding, changing, or removing information, pictures, or other data. The service providers of SNS typically have controls to contact SNS users, view their profile, add them to their list of contacts, and so on. They also need to be aware of viruses or data theft. Larger SNS, such as Facebook, often work with law enforcement to try to cover such incidents. Korea Internet and Security Agency (KISA) insists to strengthen the information privacy in the age of cloud-computing and SNS. This statement is consistent with the opinion of EU to introduce "Right to be forgotten," which means to elevate the level of legal regulation

over protection of information privacy.

'Privacy' is the right of individuals to be left alone, to enjoy autonomy, and to determine how and whether information about one's self is exposed to others (Stein and Sinha, 2002). Privacy consists of privacy of a person, personal communication privacy, personal behavior privacy, and personal data privacy (Clarke, 1999). As most communications of SNS are digitized and stored as information, we can merge personal communication privacy and personal data privacy into the construct of 'information privacy' (Belanger and Crossler, 2011). There are many definitions for information privacy. First, Smith et al. (1996) identify four dimensions: collection, unauthorized secondary use, improper access, and errors. Solove (2006) identifies another four dimensions: collection, information processing, information dissemination, and invasion. Skinner et al. (2006) propose information privacy in collaborative environments focused on time, matter, and space dimensions. Clarke defined information privacy as "the interest an influencing, the handling of data about themselves." 'Privacy concerns' can be addressed by stating that fair procedures for managing the information of SNS users will be employed (Culnan and Armstrong, 1999). 'Information privacy concerns' is privacy concern based on an information-processing theory (Hann et al., 2007).

Ⅲ. CVM and WTA

Market data are not available for public services or for services that are offered for free. In such situations, it is necessary to use a procedure that does not rely on market data. CVM has been proposed in the environmental literature for such situations (Hanemann, 1984) and is one of the most popular methods for analyzing and measuring the value of publicity (Wertenbroch and Skiera, 2002). CVM is a survey-based economic technique for the valuation of non-market goods and services. While these give peoples' utility, certain aspects of them do not have a market price as they are not directly sold. However, it would be tough to value using price-based models. CVM is one technique used to measure these aspects, and often represented as a stated preference model different from a price-based revealed preference model. CVM has been widely used by government departments when performing cost-benefit analysis of projects impacting on the environment. Now, it is widely accepted as a real estate appraisal technique, especially in contaminated property or other situations where exposed preference models fail due to disequilibrium in the market (Mundy and McLean, 1998).

Typically, CVM asks how much money people would be willing to accept (or willing to pay) to be compensated for the loss of (or maintain the existence of) a non-market goods or services feature. WTA (related to our study) is the amount of money that a user is willing to accept to abandon a good/service or to put up with something negative, such as pollution or invasion of information privacy. It is the minimum monetary amount required for the sale of a good/service or acquisition of something unwanted to be accepted by an individual. Conversely, willingness to pay (WTP) is the maximum amount anyone is willing to sacrifice to procure a good/service or avoid something undesirable. Several methods were developed to measure consumer WTP. These methods can be differentiated whether they measure consumers' hypothetical or actual WTP (and directly or indirectly). Thus, the price of any goods/ services transaction will be any point between a buyer's WTP and a seller's WTA. The net difference between WTP

and WTA is the social surplus created by the trading of goods/services. Unlike WTP, WTA is not constrained by an individual's wealth. For example, WTP to stop the ending of one's own life can be as big as one's wealth, while the WTA compensation to accept the loss of one's life would be an extremely high number.

Alternative techniques for estimating WTA have been proposed and used in the marketing literature, including the choice-based experiments, such as conjoint analysis. Although each approach has its own advantages and disadvantages, along with their own set of detractors (Diamond and Hausman, 1994; Hausman, 1993) and supporters (Hanemann, 1994), there is no consensus that any one method is clearly preferable to the other (Foster and Mourato, 2003; Hanley et al., 2001; Stevens et al., 2000). However, there is now increasing evidence that carefully designed.

Establishing CVM can be distinguished in 5 steps. Step 1 selects a research target, and defines the valuation problem and select non-market resource. Step 2 is the construction of a hypothetical market. First, the main idea is to construct a scenario which corresponds as closely as possible to a real situation. The scenario contains precisely the reason for payment with standard market goods or services, and must be understood by the respondent. Second, it constructs a method of payment that fulfills conditions with respect to incentive compatibility, realism, and subjective justice among respondents. Third, it constructs a provision rule by which the good is to be provided, as a function of the stated value.

Step 3 designs survey questionnaire. First, a CVM researcher selects a limited sample of the underlying population, and presents possible bidding mechanism. The several types of possible bidding mechanisms are open-ended question, bidding game, payment card, Dichotomous-choice (DC) question (see <Table 1>). First, bidding game asks a sequence of questions until maximum WTP or minimum WAP is found. Payment card presents average expenses of other goods per a household, and induce respondents into answering their WTP or WTA for research object. The card indicates a range of possible values, one of which is pointed out by the interviewee. Open-ended question leads the respondent directly insist their WTP or WTA without options. Dichotomous-choice (DC) question presents two kinds of methods. Single-bound dichotomous choice (SBDC) provides little information only one bound. Double bound dichotomous choice (DBDC) same as SBDC, but an additional follow-up question is required. This amount of price is previously de-

<Table 1> Bidding Mechanism Type of CVM

Method	Feature
Open-ended question	Respondents are asked to state their minimum WTA for the amenity to be valued
Bidding game	Respondents are asked a sequence of questions until maximum is found
Payment card	Respondents can be shown a payment card listing various dollar amounts and asked to circle the one that comes closest to their own value
Dichotomous-choice (DC) question	Respondents are asked if they are willing to pay a single randomly assigned amount on all-or-nothing basis (‘yes’ or ‘no’ answer)

termined by 'Open-end' method. In case of WTA, respondents are supposed to choose "NO" if the price is higher than they can accept, and choose "Yes," if not.

Step 4 conducts the survey written in Step 3. In person interviews may be conducted with random samples of respondents. Step 5 conducts the survey result analysis estimating average WTP or WTA, bid curves, and aggregating the data. The data must be entered and analyzed using statistical techniques adequate for the type of question to estimate public WTP or WTA. The application procedure of CVM is arranged in <Table 2>.

Ⅳ. Data and Measurement

Our study estimated WTA throughout CVM. Data for analyzing our study came from a survey of a research company 'Embrian' which figure out WTA by presenting respondents virtual market buying or selling personal information. 20s are younger and probably more familiar with SNS than the general population. They may have had little experience, and had too little wealth to be familiar with investment opportunities and risks. For these reasons, it would be important to verify our research with more representative sample.

This survey assumed how much compensation SNS users obtain by agreeing 'friend request' on SNS from virtual marketing firm so as to acquire precise response. Also, we estimated the value of information privacy on SNS by measuring the WTA of SNS users for 'friend request' from the virtual marketing firm. Above all, the basic scenario for this survey was to make a series of decisions in the WTA for 'friend request' of a virtual marketing firm. The survey had to be slightly altered for respectively presented compensation price. Respondents were given appropriate visual instructions for each scenario concerning 'friend request' from a virtual marketing firm. WTA responses were elicited using a DBDC question. The bids of DBDC question required respondents to evaluate their WTA given the repeated choices of whether

<Table 2> Application Procedure of CVM

Step 1. Research target selection	Define the valuation problem and select non-market resource
Step 2. Scenario selection	Create a hypothetical market
Step 3. Survey questionnaire design	Present a hypothetical scenario describing the change in the good to be valued Present the hypothetical payment mechanism and related stipulations Elicit the respondent's WTP or WTA ("bid elicitation procedure") Collect information on respondent's socioeconomic characteristics
Step 4. Survey	Preliminary survey : Provide base initial bid for the main survey Main survey : In-person interviews may be conducted with random samples of respondents
Step 5. Survey result analysis	The data must be entered and analyzed using statistical techniques appropriate for the type of question to estimate public WTP or WTA Identify possible non-response bias

the SNS user would permit 'friend request' for a presented compensation. Five distinct price ranges within the typical compensation price were utilized. Each present compensation price randomly received bids corresponding to one of the price ranges.

An important issue in CVM is one of optimal bid design. Clearly, the distribution of the chosen bids impacts the efficiency of the estimators, and should therefore be chosen after careful deliberation. A number of respondents have derived optimal bidding mechanisms (e.g., Alberini, 1995; Hanemann et al., 1991; Kanninen, 1995). In order to get optional bid prices presented in CVM survey, we conducted a pretest based 'open-end' method. We interview 30 people personally, explain about the scenario of our study, and ask them to present their WTA if they would measure the value of information privacy on SNS. In this process, we supplied enough explanations on SNS for the respondents who are lack of basic experiences and knowledge on SNS. Based on the WTA of respondents derived from pretest, we presented the various optional bid prices (20, 40, 60, 80, and 100 thousand won) required in our survey.

To develop a framework for analyzing WTA based this five bid sets, we utilized a random utility framework, such as that developed by Hanemann (1984). First, we can write the utility function of an individual *j* as

$$u_{ij=u_i}(y_j, x_j, \varepsilon_{ij})$$

where *i* takes a value of 0 for the reject for 'friend request' from the virtual marketing firm, but takes a value of 1 for the acceptance for, is respondent *j*'s discretionary income, and represents the vector of relevant covariates of the individual which might affect the utility function (e.g., age, gender, education, etc.). However, it contains some components which are unobservable to econometric investigator, thus, treated by the investigator as stochastics is unobservable components represented as the random variables with zero means.

Now, if we ask a respondent WTA won for 'friend request' from the virtual marketing firm, a negative answer implies

$$\begin{aligned}\Pr(no) &= \Pr[u_i(y_j - t_j, x_j, \epsilon_{ij}) > u_0(y_j, x_j, \epsilon_{0j})] \\ &= F(t_j)\end{aligned}$$

$$\begin{aligned}\Pr(yes) &= \Pr[u_i(y_j - t_j, x_j, \epsilon_{ij}) > u_0(y_j, x_j, \epsilon_{0j})] \\ &= 1 - F(t_j)\end{aligned}$$

Assuming additive separability of the utility function, we can specify a parametric utility function in the form of

$$u = \alpha x + \beta(y) + \varepsilon$$

and derive the following relation:

$$\begin{aligned}\Pr(no_{j)} &= \Pr[(\alpha x_j - \beta t_{j)>} - \varepsilon_j] \\ &= \Pr[\alpha x_j - \beta t_j + \varepsilon_j > 0]\end{aligned}$$

This gives us a simple way of estimating the mean WTA based on the answer to a single question (SBDC). However, this method abstracts away from the impact of income on WTA by assuming a constant marginal utility of income. To overcome this restriction, it is possible to directly model the WTA function by using a DBDC where users are asked to respond to a series of sequenced questions following the initial bid (Raghu et al., 2009). A DBDC question presents respondents with a sequence of two bids and asks them if their WTA equals or exceeds that bid. The magnitude of second bid depends on

the answer (yes or no) to the first bid. Denoting the initial bid as $B1$, a respondent would be asked whether or not the respondent would permit friend request if it were priced at $B1$. If the answer is "no," the respondent is presented with a new bid BH, such that $BH > B1$. However, if the respondent's response is positive, she is presented with $BL < B1$. Hence, the four outcomes may be represented as below. We use the CVM approach to develop our value model of information privacy on SNS.

$$(1)\ \Pr(yes-yes) = \Pr[WTA_j \le B_{1j} \text{and} WTA_j \le B_{Lj}] = F(B_{Lj})$$

$$(2)\ \Pr(yes-no) = \Pr[WTA_{j\le} B_{1j} \text{and} WTA_j > B_{Lj}] = F(B_{1j}) - F(B_{Lj})$$

$$(3)\ \Pr(no-yes) = \Pr[WTA_j > B_{1j} \text{and} WTA_j \le B_{Hj}] = F(B_{Hj}) - F(B_{1j})$$

$$(4)\ \Pr(no-no) = \Pr[WTA_{j>} B_{1j} \text{and} WTA_j > B_{Hj}] = 1 - F(B_{Hj})$$

where F () represents the cumulative distribution function (cdf). Equations (1)-(4) represent the probabilities of observing the different response to each of the individual bids and yield the likelihood function for estimating the mean WTA for the sample. Consequently, equations (1)-(4) yield the following sample log-likelihood function:

$$\begin{aligned} ln\mathrm{L} = {} & \sum_{i=0}^{n}[(yes-yes)\ln F(\frac{BLi-\xi\beta}{\sigma}) \\ & +(yes-no)\left\{\ln[F\left(\frac{B_{1i}-x_i\beta}{\sigma}\right)-F\left(\frac{B_{Li}-x_i\beta}{\sigma}\right)]\right\} \\ & +(no-yes)\left\{\ln[F\left(\frac{B_{Hi}-x_i\beta}{\sigma}\right)-F\left(\frac{B_{1i}-x_i\beta}{\sigma}\right)]\right\} \\ & +(no-no)\left\{\ln[1-F\left(\frac{B_{Hi}-x_i\beta}{\sigma}\right)]\right\} \end{aligned}$$

A variety of distributions, such as the lognormal, normal and Weibull, have been suggested for modeling WTA. The parameters of these distributions can be specified as functions of covariates. The vectoris operationalized using specific control variables and relevant covariates. The coefficient estimates reveal the marginal impact of these covariates on WTA and the mean WTA for the sample is estimated as E (WTA) = β in spike model. The spike model basically uses additional valuation questions: 1 asks whether or not the individual would want to contribute at all to this survey. Thus, it takes into account a spike at zero WTA which is the truncation at 0 of the positive parts of the WTA distribution. Here, spike is defined by:

$$F(t_j) = \frac{1}{1+\exp(\alpha)}$$

representing the percentage of respondents' zero WTA among samples and mean WTA is estimated as:

$$WTA_{mean} = \frac{1}{\beta} ln(1+\exp(\alpha))$$

The five bid sets were in the 10 - 200 thousand won range as follows: (20, 10, 40), (40, 20, 80), (60, 30, 120), (80, 40, 160) and (100, 50, 200), where each number represents (bid 1, subsequent lower bid, subsequent higher bid). Based on the response, the next higher bid is presented if the response is "no," or the next lower bid is presented if the response is "yes."

Then, we present more specific questions like how the respondents use SNS and how frequently they the level of satisfaction. WTA is often impacted by individual attitudes and demographic characteristics. WTA survey collected several covariates for later incorporation into the model. We collected demo-

graphic information including age, gender, education, monthly expenditure, years of experience using SNS, and number of hours or frequency of SNS use each day. SNS uses an ability. SNS satisfaction level, privacy invasion experience, and perceived security level of respondents on SNS were checked by a five-point scale item. We also conducted to other measures of SNS friend number and structure of SNS. A variety of techniques, such as CVM and logit models, are proposed to measure the compensation or WTA for information privacy on SNS. These measurements require respondents to evaluate relative to information privacy that exist on SNS.

This survey was conducted through on-line in October, 2014. We checked whether respondents followed the sequence of questions given in the DBDC. Responses that did not follow the sequence correctly were removed from the final sample. Data for the complete study were collected from a population of 312 respondents. Descriptive statistics for the data used in this study are presented in <Table 4>. <Table 4> reports the estimated mean WTA values for each of the 14 conditions. This left us with a final sample of 312 respondents – 50.32% were male; the average age was 39.23 years; college is the most of Education; and the average monthly expenditure is 1,594 thousand won.

Ⅴ. Results

Our study investigated the sensitivity of information privacy on SNS through 14 conditions (about SNS feature and characteristic of SNS users). Since we have limited dependent variable that has only 4 ordinal stages, i.e., yes-yes, yes-no, no-yes, no-no, it would not be appropriate to use ordinary least square. In statistics, the ordered logit model (also ordered logistic regression or proportional odds model) is being used for ordinal dependent variables. For example, if one question on a survey is to be answered from a choice among "poor," "fair," "good," "very good," and "excellent," and the purpose of the analysis is to see how well that response can be predicted by the responses to other questions, some of which may be quantified, then ordered logistic regression may be used. Therefore, we adopted an ordered logit regression, and <Table 2> shows the regression results for information privacy on SNS.

The characteristic of SNS users consists of satisfaction level, perceived security level, use ability, and experience of privacy invasion on SNS. As the SNS feather, there is a type of SNS whether it is close-based or open-based.

In demographic variable, education shows 5% significant level and B value of 0.211. Thus, the higher is education, the higher is WTA. This implicates those who have a high level of education are more sensitive to information privacy on SNS. In SNS usage cycle variable, year of experience using SNS shows 5% significant level and B value of -0.155. Thus, the longer is year of experience using SNS, the lower is WTA. This implicates those who have long-time experience on SNS are less sensitive to information privacy.

This result is quite surprising to us. We originally thought that those with long experience of SNS, or those who heavily use SNS would have very high information privacy concern because they have disclosed too much information on the Web. So, their valuation of information privacy would be very high. However, we found the opposite result, so that heavy users have lower information privacy value. We surmise that this is due to the reverse causality. In other words, they heavily use SNS and disclose so much information because their information privacy con-

<Table 3> Descriptive Statistics

Variable	Statistics		Mean	Standard Deviation
Age	The twenties and less = 63 The forties = 81	The thirties = 94 more than the fifties =74	39.23	10.712
Gender	Male = 157	Female = 155	-	-
Education	High school and less = 70 College = 170	Junior college = 47 more than Graduate = 25	3.48	0.935
Monthly expenditure	50 and less = 91 100~200 = 82	50~100 = 61 more than 200 = 78	159.38	132.262
Year of experience using SNS	1 year and less = 47 2~3 year = 91 more than 4 year = 62	1~2 year = 65 3~4 year = 47	3.04	1.327
Hours of SNS use each day	10 min. and less = 101 30~60 min. = 54 more than 2 hour = 15	10~30 min. = 116 1~2 hour = 26	2.16	1.114
Frequency of SNS use each day	1 and less = 86 6~10 = 50 more than 21 = 30	2~5 = 117 11~20 = 29	2.36	1.245
Type of SNS	Closed type = 172	Open type = 140	-	-
The number of SNS friend	20 and less = 83 50~100 = 51 more than 200 = 30	20~50 = 93 100~200 = 55	135.98	596.126
The number of SNS event join	0 = 123 more than 6 = 53	1~5 = 136	3.94	12.496
Experience of privacy invasion	1 level = 41 3 level = 120 5 level = 2	2 level = 116 4 level = 33	2.19	0.78
Satisfaction level of SNS	1 level = 0 3 level = 105 5 level = 16	2 level = 13 4 level = 178	3.63	0.648
Perceived security level of SNS	1 level = 35 3 level = 33 5 level = 4	2 level = 216 4 level = 24	2.19	0.78
Use ability of SNS	1 level = 4 3 level = 131 5 level = 24	2 level = 56 4 level = 97	3.26	0.886

cern is quite low.

In SNS feature variable, type of SNS shows 10% significant level and B value of -0.386. This implicates those who use open-based SNS are less sensitive to information privacy. This result is also similar to the above explanation. People with high information privacy concern would not use open-based SNS and would use only closed SNS.

In the character variable of SNS users, perceived security level of SNS users shows 5% significant level and B value of 0.333. Thus, the higher is perceived security level of SNS users, the higher is WTA. This implicates those who have security consciousness are more sensitive to information privacy on SNS. In contrast, the satisfaction level of SNS users shows 5% significant level and B value of -0.329. Thus, the higher is the satisfaction level of SNS users, the lower is WTA. This implicates those who are satisfied with SNS in use are less sensitive to information privacy on SNS. Also, the use ability of SNS shows

<Table 4> Ordered Logit Model Results for Information Privacy on SNS

Variable	*B*	Standard Error	Wald	*P*-value
Constant	2.219	.999	4.935	.026**
Bid	-1.246E-05	3.593E-06	12.023	.001***
Age	-.010	.010	1.035	.309
Gender	.083	.197	.178	.673
Education	.211	.105	4.084	.043**
Monthly expenditure	.000	.001	.031	.860
Year of experience using SNS	-.155	.078	3.961	.047**
Hours of SNS use each day	-.021	.110	.038	.846
Frequency of SNS use each day	.103	.107	.926	.336
Type of SNS	-.386	.214	3.259	.071*
The number of SNS friend	8.750E-05	.000	.297	.586
The number of SNS event join	.001	.008	.025	.874
Experience of privacy invasion	.114	.119	.915	.339
Satisfaction level of SNS	-.329	.167	3.896	.048**
Perceived security level of SNS	.333	.136	6.034	.014**
Use ability of SNS	-.234	.121	3.747	.053*
-2 Log Likelihood: 728.823	Cox & Snell : 0.117 Nagelkerke : 0.128			

Note: Dependent variable: 4 ordinal stages of WTA
Significant at 1%*** 5% **, and 10%* respectively

10% significant level and B value of -0.234. Therefore, the higher is the ability, the lower is WTA. This implicates those who make good use of SNS are also less sensitive to information privacy on SNS.

The last step for evaluating WTA is to compute the average of 14 conditions on the value of information privacy on SNS. WTA mean is 173,957 won /number in <Table 5>. To compute the information privacy value of the whole SNS users, we expanded the value of sample to the information privacy value of total SNS users. Using this mean WTA, we can estimate information privacy value of all users for an SNS firm. For example, we may apply this figure into Facebook. Considering that there are 11 million users in Korea, we can say that the total value of privacy for Korean users would be 1.91 trillion won.

Ⅵ. Conclusion

Our study investigated the sensitivity of information

<Table 5> WTA Estimation for Information Privacy on SNS

Variable	B (A)	Mean (B)	A * B
Constant (b)	2.219		
Bid	-1.246E-05		
Age	-.010	10.712	-0.10760
Gender	.083	0.501	0.04162
Education	.211	0.935	0.19764
Monthly expenditure	.000	132.262	-0.01753
Year of experience using SNS	-.155	1.327	-0.20599
Hours of SNS use each day	.-021	1.114	-0.02393
Frequency of SNS use each day	.103	1.245	0.12876
Type of SNS	-.386	0.498	-0.19228
The number of SNS friend	8.750E-05	596.126	0.05216
The number of SNS event join	.001	12.496	0.01508
Experience of privacy invasion	.114	0.875	0.09956
Satisfaction level of SNS	-.329	0.648	-0.21353
Perceived security level of SNS	.333	0.780	0.25991
Use ability of SNS	-.234	.886	-0.20698
Total (a)			2.04541
Mean WTA	173,957	$\frac{1}{b}ln(1+\exp(a)$	

<Table 6> Correlation Matrix of 14 Conditional Variables for Information Privacy on SNS

	Age	Gender	Education	Monthly expenditure	Year of experience using SNS	Hours of SNS use each day	Frequency of SNS use each day	Type of SNS	The number of SNS friend	The number of SNS event join	Experience of privacy invasion	Satisfaction level of SNS	Perceived security level of SNS	Use ability of SNS
Age	1													
Gender	.164**	1												
Education	.010	.089	1											
Monthly expenditure	.279**	.038	.087	1										
Year of experience using SNS	-.100	.068	.006	.005	1									
Hours of SNS use each day	-.055	.068	-.052	.019	.274**	1								
Frequency of SNS use each day	-.200**	-.033	-.109	-.038	.373**	.638**	1							
Type of SNS	-.214**	.149**	.029	-.274**	.057	.009	.035	1						
The number of SNS friend	.055	.077	.001	-.061	.128*	.218**	.200**	.111*	1					
The number of SNS event join	.026	-.004	-.039	-.048	.094	.204**	.162**	.061	.242**	1				
Experience of privacy invasion	.101	.132*	.000	-.006	.136*	.224**	.191**	.127*	.085	.131*	1			
Satisfaction level of SNS	.060	.127*	-.101	-.016	.110	.278**	.300**	-.213**	.066	.062	-.008	1		
Perceived security level of SNS	.178**	-.100	-.060	-.004	-.168**	-.142*	-.225**	-.058	-.053	.077	-.099	-.125*	1	
Use ability of SNS	-.135*	.038	-.057	-.094	.262**	.254**	.376**	.121*	.109	.082	.302**	.195**	-.163**	1

privacy on SNS through 14 conditions (about SNS feature and characteristic of SNS users). We estimate WTA throughout DBDC. As a result of our study, while the use rate of SNS increased rapidly, sensitive SNS users for information privacy have following characteristics: higher education, less SNS experience, and higher security consciousness. Contrarily, those who make good use of SNS and those who use open-based SNS are less sensitive to information privacy. Overall, we were able to find that the sensitive SNS users for information privacy feel fearful or uneasy when they are not good at controlling SNS information.

In consideration of 14 conditions on the value of information privacy on SNS, the mean value of SNS information per person is 173,957 won. This means that a typical user may share his or her personal information with others if that much money would be given. If we apply this figure into Facebook, we can say that the total Facebook information value would be 1.91 trillion won considering there are 11 million users in Korea.

Our study has contributions both academically and practically. Academically, our paper tried to figure out the factors that affect the value of information privacy on SNS. To our understanding, this is the first study to empirically measure the actual value of privacy concern on SNS. Combining privacy literatures in information system researches together with contingent valuation methods in economics, we believe that we extended the horizon of privacy studies one step further. Our results may help SNS users figure out the factors that affect the value of information privacy and how importantly they perceive the information privacy of themselves on SNS. Our finding implies that SNSs may possess means to actively manage the information privacy concerns of users. Our results also suggest that SNSs may alleviate privacy concerns by increasing protection efforts and also they may provide financial incentives to collect more online information.

Regarding managerial implications, our findings are worthy of notice for practitioners that provide and operate SNS or managers who want to use SNS as a marketing channel. Most of SNS don't suggest an enough explanation on the protection of information privacy, but our study leads to enlighten SNS users who show worry or unconcern about information privacy. Recently, closed-based SNS, such as KakaoStory and Band, grow rapidly, while the growth rate of open-based SNS is tied up. This might be due to increasing privacy concerns in open-based SNS. This phenomenon matches up with our result nicely. Namely, if SNS firms provide enough tools to protect information privacy, SNS firms may more appeal SNS users who are sensitive to information privacy.

This paper would help us figure out the factors that affect the value of information privacy and derive implications for information privacy administration on SNS. We conducted this approach because there have been no literature about how important a user perceives information privacy on SNS and the official market to sell personal information has never been formed. We made the results on the value of information privacy on SNS more persuasive by analyzing an ordinal multinomial regression model.

There are a few limitations in our study. Basically WTA has a bit of perceived problems with protest bids and infinitely-high bids. Furthermore, WTA is possible that there is always a population of users who absolutely refuse 'friend request,' i.e., their WTA is zero (a subject with a zero WTA would answer "no-no-no" to the sequence of three WTA bids). We didn't obtain a response to the WTA bids with "no-no-no" in CVM. Nevertheless, these problems

can be complemented through further studies in the future. Another limitation of our study is that our finding is basically correlation rather than causality. Our result that heavy SNS users have lower a value of their information might be due to the reverse causality. In other words, those who have low values of their information use SNS much heavily. Clarifying the causality relationship would be remaining for future studies.

<References>

[1] Bélanger, F. and Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly, 35*(4), 1017-1042.

[2] Boyd, D. (2007). *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*. MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume (ed. David Buckingham). Cambridge, MA: MIT Press.

[3] Boyd, D. M., and Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication, 13*(1), article 11, Retrieved 2012-01-30.

[4] Clarke, R. (1999). Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM, 42*(2), 60-67.

[5] Culnan, M. J., and Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*(1), 104-115.

[6] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. (2006). Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States. *Journal of Global Information Management, 14*(4), 57-93.

[7] Diamond, P. A., and Hausman, J. A. (1994). Contingent Valuation: Is Some Number better than No Number? *The Journal of Economic Perspectives, 8*(4), 45-64.

[8] Hann, I. H., Hui, K. L., Lee, S. Y. T., and Png., I. P. (2007). Overcoming Online Information Privacy Concerns: An Information- Processing Theory Approach. *Journal of Management Information Systems, 24*(2), 13-42.

[9] Hanemann, W. M. (1984). Welfare Evaluation in Contingent Valuation Experiments with Discrete Responses. *American Journal of Agricultural Economics, 66,* 332-341.

[10] Hanemann, W. M. (1994). Valuing the Environment Through Contingent Valuation. *Journal of Economic Perspectives, 8*(4), 19-43.

[11] Hausman, J. A. (1993). *Contingent Valuation: A critical Assessment, Amsterdam*. North Holland Press.

[12] Heylighen, F. (2007). *Why is Open Access Development so Successful? Stigmergic Organization and the Economics of Information*. In B. Lutterbeck, M. Barwolff, and R. A. Gehring (Eds.), Open Source Jahrbuch Media.

[13] Lohr, S. (2010). http://www.nytimes.com/2010/03/17/technology/17privacy.html, 'How privacy vanishes online', March 16, 2010.

[14] Mackaay, E. (1990). Economic Incentives in Markets for Information and Innovation. *Harvard Journal of Law and Public Policy, 13*(909), 867-910.

[15] Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355.

[16] McLean, I. and McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3rd ed.). OUP Oxford.

[17] Milberg, S. J., Smith, H. J., and Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science, 11*(1), 35-57.

[18] Mundy, B. and McLean, D. (1998). Using the Contingent Value Approach for Natural Resource and

Environmental Damage Applications. *The Appraisal Journal, July,* 88-99.

[19] Raghu, T. S., Sinha, R., Vinze, A. and Burton, O. (2009). Willingness to Pay in an Open Source Software Envirnment. *Information Systems Research, 20*(2), 218-236.

[20] Rosenblum, D. (2007). What Anyone Can Know: The Privacy Risks of Social Networking Sites. IEEE *Security and Privacy, 5*(3), 40-49.

[21] Schaar, A. K., Valdez, A. C., and Ziefle, M. (2013). *The Impact of User Diversity on the Willingness to Disclose Personal Information in Social Network Services.* In Human Factors in Computing and Informatics, Springer Berlin Heidelberg, 174-193.

[22] Skinner, G., Han, S., and Chang, E. (2006). An Information Privacy Taxonomy for Collaborative Environments. *Information Management and Computer Security, 14*(4), 382-394.

[23] Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly, 20*(2), 167-196.

[24] Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477-564.

[25] Stein, L., and Sinha, N. (2002). *New Global Media and Communication Policy: the Role of the State in Twenty-First Century, in L. Lievrouw and S. Livingstone* (Eds.), Handbook of New Media: Social Shaping and Consequences of ICTs, London: Sage, 410-431.

[26] Stewart, K. A., and Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research, 13*(1), 36-49.

[27] Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. (2006). Concern for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems, 7*(6), 415-444.

[28] Wallbridge R. (2009). How Safe is Your Facebook Profile? Privacy Issues of Online Social Networks. *ANU Undergraduate Research Journal, 1.*

[29] Wertenbroch, K., and Skiera, B. (2002). Measuring Consumers' Willingness to Pay at the Point of Purchase. *Journal of Marketing Research, 39*(2), 228-241.

◆ About the Authors ◆

Woo-Jin Jung

Woo-Jin Jung is in a post-doctoral research in School of Information, Yonsei University, Seoul, Korea. He received his Ph.D. degree in MIS from Hanyang University, Seoul, Korea (2015). His research interests are in the area of Privacy and Information Security, IT value measurement, and R&D performance measurement. His papers have been published in Asia Pacific Journal of Information Systems, Journal of Information Technology Applications & Management and Telecommunications Review.

Sang-Yong Tom Lee

Sang-Yong Tom Lee is a Professor in School of Business, Hanyang University, Seoul, Korea. He was on the faculty of Department of Information Systems, National University of Singapore before joining Hanyang University. He received his Ph.D degree from Texas A&M University (1999). His research interests include economics of information systems, online information privacy, and value of IT. His papers have been published in Management Science, MIS Quarterly, Journal of Management Information Systems, Communications of the ACM, IEEE Transactions on Engineering Management, Information and Management, and others.

Submitted: December 31, 2014; 1st Revision: March 31, 2015; Accepted: May 13, 2015