Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2017 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 2017

Estimating the Monetary Value of Information Privacy in the Context of SNS

Woojin Jung
Yonsei University, hygm2003@gmail.com

Hee-Woong Kim
kimhw@yonsei.ac.kr

Estimating the Monetary Value of Information Privacy in the Context of SNS

Completed Research Paper

Woo-Jin Jung
Graduate School of Information,
Yonsei University
Seoul, Korea
hygm2003@gmail.com

Hee-Woong Kim
Graduate School of Information,
Yonsei University
Seoul, Korea
kimhw@yonsei.ac.kr

Abstract

The dramatic growth of SNS has created a myriad of information privacy. To achieve our objective, first, this study estimates the monetary value of information privacy by using the CVM. Second, it is estimated how the monetary value of information privacy would change according to demographic information, SNS usage cycle information, the Characteristics of SNS users, and the SNS features. As a result, sensitive SNS users for information privacy have following characteristics: 30s, higher education, less Monthly Expenditure or far more monthly expenditure, lower SNS use ability, more number of followers, little event experiences, shorter SNS experience, higher account open limit level and privacy invasion experiences. Also, the total WTA mean is $28/number. The monetary value of information privacy according to SNS features have the following characteristics. Those who use private SNS, the value of Profile, Location information, and the purpose of Sharing and Friendship are more important.

Keywords: SNS, CVM, WTA, Information Privacy, Logistic Regression Model

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. It is designed to form new networks and strengthen relationships with others. Especially, SNSs 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. The dramatic growth of SNS has created a number of privacy concerns. Privacy concerns are much more noticeable in SNS than other media such as personal websites like blogs. SNS users are not sufficiently aware of these privacy concerns. The attributes of SNS user can be classified into three parts; privacy guardians, information sellers, and convenience seekers (Hann et al. 2007). 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 fashionable but also popular 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, that is, SNS users can select who may see their page, allow only him or her added as 'friends' to view their profile, and prevent undesirable viewing of the profile by other users. They are trying to create a structural obstacle between their privacy and 'friends' addition. Nevertheless, privacy concerns on SNS can be undermined by many factors. For example, SNS users can disclose the information about themselves, SNS cannot take adequate steps to protect the information of SNS users, and third parties frequently can use information about SNS users posted on SNS for a variety of purposes (Rosenblum 2007).

Studies on privacy concern typically seek 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 (Smith et al. 1996; Milberg et al. 2000; Stewart & Segars 2002; Malhotra et al. 2004; Dinev & Hart 2006; Van Slyke et al. 2006).

They found that privacy concerns differ between SNS users according to sex and personality (Schaar et al. 2013). For example, women are less likely to invade information privacy; openness, extraversion, and conscientiousness were found to positively affect the willingness to expose data, while neuroticism decreases the willingness to expose information (Schaar et al. 2013). Also, they found that SNS users would rather present their information than being anxious, when the provision of personal information could be economically rewarded by SNS (Hann et al. 2007). This personal information on SNS 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 use value of SNSs has not been established in users' minds.

The psychological concept of 'Privacy' includes a wide variety of definitions (Margulis 1977). It emphasizes privacy as control over or regulation of or limitations on or exemption from scrutiny, surveillance, or unwanted access (Allen 1988; Margulis 1977). Many researchers view privacy neutrally because they believe privacy can support illegitimate activities, such as misuse of a public office (Westin 1967) and vandalism (Altman 1975), and morally dubious behavior like lying (Derlega & Chaikin 1977). The recent examination evaluates privacy theories of Altman's (1975) and Westin's (1967). The privacy theory of Altman (1975) focuses on privacy as a process of regulating levels of social interaction, and that of Westin (1967) focuses on the states (types) and functions of privacy. The principal difference is that Altman's theory is relatively inclusive of privacy phenomena but Westin's theory is less so, often focusing on information privacy.

Information privacy is a very current and exciting study domain that will continue to evolve as new technologies and new initiatives (Bélanger & Crossler 2011). Even with the importance of this topic, there has been little study on estimating the monetary value of information privacy. This research thus aims to estimate the monetary value of information privacy in the SNS context. Especially, it focuses on estimating how much money SNS users want to accept for disclosing their SNS information by accepting

friend offer. To achieve this research objective, first, this study focuses on the matter of information privacy caused by SNS, and estimates the willingness to accept (WTA) value of information privacy, non-rival good, by using the contingent valuation method (CVM) which is an influential method to evaluate stated preference (Hanemann 1984; Wertenbroch & Skiera 2002). Second, it is estimated how the WTA value would change when demographic information (including gender, age, education, employment, monthly expenditure), SNS usage cycle information (including use frequency a day, use duration at a time, and use period) as well as the Characteristics of SNS users (including event participation number, follower number, SNS use ability). Additionally, this study identifies whether the monetary value of information privacy changes according to the SNS features (SNS firm, SNS type, the type of SNS information, the purpose of SNS use).

This research estimates the value of information privacy on SNS more persuasively by analyzing an ordered logistics model, and contributes to the literature by figuring out the factors that affect the monetary value of information privacy and providing implications for information privacy administration on SNS. This review is organized as follows: discussing the literature of SNS and information privacy concerns on SNS is begun. Then, data and methodology (including a description of the CVM and WTA) are presented. Having done that, the results of our empirical findings are discussed. Finally, based on our results, a new focus for the future research is suggested.

What is the Information Privacy?

The privacy concept of Westin (1967) is defined as "the ability of the individual to control the terms under which personal information is acquired and used". Then *information privacy* refers to "the ability of the individual to personally control information about one's self" (Stone et al. 1983). Previous research has suggested that issues of informational control are essential in creating a favorable users' predisposition toward contributing information to online firms (Stewart & Segars 2002).

Many theories of privacy posit that psychological *control* is a precondition for obtaining and maintaining privacy (Altman 1975; Johnson 1974; Wolfe & Laufer 1974). Adopting such a control perspective, privacy theorists argue that the loss of control over personal information is central to the notion of privacy invasion. Some empirical studies provide evidence that control is a key factor that explains individual perceptions of privacy invasion (Sheehan & Hoy 2000). Malhotra et al. (2004) posit that control is one of the most important factors affecting privacy concerns among Internet users. People tend to perceive information disclosure as less privacy-invasive if they believe that they have control over the collection and use of their personal information (Culnan & Armstrong 1999). Johnson (1974) defined privacy as "secondary control in the service of need-satisfying outcome effectance". Also, Goodwin (1991) defined customer privacy by two dimensions of control: control over information disclosure and control over unwanted physical intrusions into the customer's environment. Privacy should be more than control and control might be one of the factors which determine privacy state (Laufer & Wolfe 1977). These considerations suggest that perceived control over disclosure and subsequent use of personal information is a separate construct from privacy concerns and that the two constructs are negatively related. Prior research has shown that individuals will have fewer privacy concerns when they have a greater sense that they control the disclosure and subsequent use of their information (Milne & Boza 1999).

The benefits of privacy reflect privacy's functions. Privacy protects personal autonomy and provides opportunities for people and organizations to prepare and discuss matters "in private"; it allows non-political participation in family, religion, and in other forms of association (Westin 1967). The costs of privacy arise from failures to obtain or maintain privacy. However, the benefits and costs are predicted or potential, rather than demonstrated. Not obtaining privacy could result in the loss of opportunities that the functions of privacy provide. They are lost because people fail to psychologically control privacy-related behaviors (Johnson 1974). When privacy is invaded or violated, it is lost. Invasions occur when initial conditions for privacy are not achieved. Violations of privacy occur when recipients disclose to others the private information intentionally shared with them or which they obtained through an invasion of privacy. Invasions and violations of privacy result in anticipated and actual

consequences (or costs) of having one's private information in the wrong hands. Costs vary considerably, depending on many factors, especially the content of the information (Margulis 1979; Johnson 1974).

Many discussions of privacy emphasize it as a positive in the sense that privacy protects behavior which is either morally neutral or valued by society (Warren & Laslett 1977). Regan (1995) observes that privacy is a social value because it supports and is supported by a democratic political system, and the public agree that the important threats to privacy have arisen from organization-individual relationships. Westin (1967) describes three empirically differentiated positions on privacy the public holds. The high-privacy position assigns a higher value to privacy claims and seeks comprehensive governmental interventions to protect privacy (see Bennett 1995; Lyon & Zureik 1996). The balanced-privacy position values privacy claims but advocates tailored governmental interventions to address demonstrated abuses as well as voluntary organizational initiatives to promote individual privacy (see Etzioni 1999; Westin 1967). The limited-privacy position usually assigns a lower value to privacy claims than to business efficiency and societal protection interests and it opposes governmental intervention as unnecessary and costly (see Singleton 1998).

Privacy is important because it is posited to provide experiences that support normal psychological functioning, stable interpersonal relationships, and personal development (Westin 1967). Personal experiences guide behavior in activities that can be subjectively deemed as privacy-related (Bates 1964). In addition, personal experiences cause a change in privacy concern over an individual's lifetime (Harris 1991). This study examines previous experience like online privacy invasion. People who have previously had their privacy invaded may not place much value on the expected outcome of useful personalization. This decreased value of personalization may result in a decreased willingness to partake in online profiling. Therefore, previous privacy invasion experience could affect an individual's concern for privacy (Culnan 1993). Users with previous privacy invasion experience have a lower willingness to be profiled online for personalized advertising. However, such a result does not hold true with regard to online service (Awad & Krishnan 2006).

There is growing concern regarding the use of information given online in terms of the privacy of personal information and the unintended uses of it (Gueutal & Stone 2005; Hunt et al. 2005; Safire 2005; Stone & Stone 1990). Effective use of personal information is a critical success factor on SNS firms. They are facing a paradox, as customers who value information transparency features are less likely to participate in personalized offerings (Awad & Krishnan 2006). There is a segment of customers that are unwilling to participate in online personalization regardless of the privacy features implemented by the firm (Awad & Krishnan 2006). From SNS marketing perspective, firms may attempt to offer value-added services to customers, so that they will overlook previous negative experiences. In addition, it may be important for firms to communicate the value of the personalization outcome to the customers in order to encourage them to partake in online personalization (Awad & Krishnan 2006). Personalized service is becoming increasingly valuable to customers and firms (Awad & Krishnan 2002). However, investments in personalization may come at the cost of customer privacy. Therefore, privacy has become an issue of strategic importance for companies operating in the information-centric global economy. In order to provide customer-driven personalized service, firms must target customers who are willing to provide information (Awad & Krishnan 2006). Thus, the perceived benefit of personalization affects the importance of previous privacy (Awad & Krishnan 2006). Previous privacy invasion is significant. It is not significant, however, as the potential benefit of the service outweighs the potential risk of a privacy invasion. Thus, companies must focus on reducing such perceived risk through implementing various online features.

Features of the SNS

SNS is a 'platform' to build social networks among people who share interests, activities, backgrounds or real-life connections (Bomil 2013). It is also '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 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 & 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 customers can use information gathered from SNS for purposes other than what users intend.

There are two types of SNS (open SNS and private SNS). Open SNS revolved around online networking, which can lead to offline interactions, and the major ones are Facebook and Twitter. Users with similar interests can get closer to each other by posting comments and photos on a theme of their interest through the system of forming ties through online search. Private SNS allows users to get closer to people, which they already know and major ones are Kakao-Talk and BAND. Private SNS revolves around communication and ties, instead of contents (Kim & Pan 2014). People who use both open SNS and private SNS were selected among different age groups for comparison with seniors in terms of user behavior. Open SNS has the following problems: invasion of privacy due to leakage of personal information; excessive exposure to unnecessary information. As a result, more and more users opted for private SNS. In particular, seniors had the most complaints about the problems of open SNS, leading to the highest popularity of private SNS among seniors (Kim & Pan 2014).

The ability to collect, analyze, and respond to SNS user information is of growing importance. To survive, firms depend on vast quantities of information to build rapport with existing customers and attract new business (Culnan & Armstrong 1999). SNS firms must use customer information to attempt to offer personalized service that will increase value and consequently, customer loyalty. However, implicit in the collection of customer information is a concern for customer privacy. *Information privacy* is one of the most important issues facing management practice (Mason 1986; Safire 2002). Previous research has found that monetary incentive affects customer preferences for privacy (Hann et al. 2002; Milne & Gordon 1993). Similarly, information requests affect the risk side of the privacy tradeoff, and hence should reduce the extent of customer disclosure (Hine & Eve 1998; Nowak & Phelps 1997; Phelps et al. 2000). Because customer information is requested in most online transactions, it is worthwhile to assess its impact in this study. SNS users have reasons to be concerned about their privacy. The top and foremost privacy problem is that SNS do not inform users of the dangers of divulging their personal information. Even if they want to protect their privacy, with too much data and too many friends, it is very difficult for users to control who can see what on their profile pages. The second problem is that privacy tools in SNS are not flexible enough to protect user data. Most SNS only allow users to make their data either public (available for everyone) or private (available only for friends) the whole profile but not every part of it. Facebook is one of the few SNS that provide very detailed privacy settings. However, the current Facebook privacy interface is too complex to most normal users. The third problem is that when users of SNS can control access to their own profile, they cannot control what others reveal about them. It is possible for information to be passed on without one's consent. For instance, a user can upload an embarrassing photo of a friend; this photo can also be tagged directly to a friend's profile.

Information on SNS is related to *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, and 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. It would be more important 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*.

CVM and WTA

It is necessary for this study to use a procedure that does not rely on market data available for public services or for services which are offered for free. 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 & Skiera 2002). CVM is a survey-based economic technique for the valuation of non- rival (or non- market) goods and services. While these goods and services give peoples utility, some aspects of them do not have a market price as they are not directly sold. Thus, it would be tough to value using price-based models. It is one technique used to measure these aspects, and often represented as a stated preference model different from a price-based revealed preference model. It 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 & McLean 1998). This study using CVM may be only in IS field.

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-rival goods or services feature. WTA (related to this 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, leakage or invasion of information privacy. It is also 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 customer WTP. These methods can be differentiated whether they measure customers' hypothetical or actual WTP. 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.

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 & Hausman 1994; Hausman 1993) and supporters (Hanemann 1994), there is no consensus that any one method is clearly preferable to the other (see Foster & Mourato 2003; Hanley et al. 2001; Stevens et al. 2000). However, improved techniques for estimating WTA are evolving continuously.

There are five steps in the application of CVM. Step 1 selects a research target, defines the valuation problem and selects non-rival resource. Step 2 is the construction of a hypothetical market. There are three ways (sub-steps or issues) for the construction. 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 some 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. In detail, 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 questions, bidding game, payment card, Dichotomous-choice question [Table 1 references]. 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 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 determined by 'Open-end' method. In case of WTA, respondents are supposed to choose "Yes" if the price is higher than they can accept, and choose "No", if not.

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 the 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)

Step 4 conducts the survey written in Step3. In person interviews may also 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.

Table2: 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 respondents' 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 results 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

Data and Measurement

This study estimates WTA based on the application of CVM. For the collection of data, this study conducted a survey in a collaboration with a survey company to figure out WTA by presenting respondents virtual market permitting or rejecting personal information exposure in the SNS context. Data was collected from the Korean SNS users by considering the most popular SNSs (Facebook, Twitter, Kakao-Talk, Band and so on) in Korea.

The survey of this study assumed how much compensation a SNS user obtains by permitting own personal information exposure on SNS for the 'friend request' of a virtual marketing firm so as to acquire accurate response. Above all, the basic scenario for this survey was to make a series of decisions in the presented compensation price for 'friend request' of a virtual marketing firm. The survey had to be slightly altered for respectively compensation prices. Respondents were given appropriate visual instructions for each scenario concerning 'friend request' from a virtual marketing firm. WTA responses were elicited using DBDC question. The bids of DBDC question required respondents to evaluate their WTA given the choice of whether the SNS user would permit 'friend request' of a virtual marketing firm for a presented compensation price. The ranges of five bids 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. 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 (see Hanemann et al. 1991, Alberini 1995, Kanninen 1995). In order to get this optional compensation prices presented in CVM survey, a pretest based 'open-end' method was conducted. 30 people personally was interviewed, explained about the scenario of this study, and asked to present their WTA for 'friend request' of a virtual marketing firm. In this process, enough explanations on SNS were supplied for the respondents who are lack of basic experiences and knowledge on SNS. Based on the WTA of respondents derived from pretest, the various optional bid sets required in this survey were presented as \$20, \$40, \$60, \$80, and \$100.

To develop a framework for analyzing WTA based on this five bid sets, a random utility framework such as that developed by Hanemann (1984) was used. First, it can be written by 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 a virtual marketing firm, but takes a value of 1 for the acceptance for, y_j is respondent *j*'s discretionary income, and $x_j$represents the vector of relevant covariates of the individual which might affect the utility function. (e.g., age, gender, education) However, it contains some components which are unobservable to econometric investigator treated by the investigator as stochastic. ε_{ij} is unobservable components represented as the random variables with zero means. Now, if a respondent is requested WTA t_j for 'friend request' from the virtual marketing firm, a negative answer implies

$$\Pr\,(no) = \Pr\,[u_i\,(y_j - t_j, x_j, \, \varepsilon_{ij}) \, > \, u_0\,(y_j, x_j, \, \varepsilon_{0j})] = F(\, t_j)$$

$$\Pr\,(yes) = \Pr\,\left[u_i\,\left(y_j - t_j, x_j, \, \varepsilon_{ij}\right) > \, u_0\,\left(y_j, x_j, \, \varepsilon_{0j}\right)\right] = \, 1 - \, F(\, t_j)$$

Assuming additive separability of the utility function, a parametric utility function can be specified in the form of

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

and derive the following relation:

$$\Pr\,(no_j) = \Pr\,[(\, \alpha\, x_j - \, \beta\, t_j) > \, -\varepsilon_{\,j}]$$

$$= \Pr\,[\, \alpha\, x_j - \, \beta\, t_j + \, \varepsilon_{\,j} > 0]$$

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 B_1, a respondent would be asked whether

or not the respondent would permit friend request if it were priced at B_1. If the answer is "no," the respondent is presented with a new bid B_H, such that $B_H > B_1$. However, if the respondent's response is positive, she is presented with $B_L < B_1$. Hence, the four outcomes may be represented as. We use the CVM approach to develop our value model of information privacy on SNS.

(1) $\Pr(yes - yes) = \Pr[\mathrm{WTA}_j \leq \mathrm{B}_{1j} \text{ and } \mathrm{WTA}_j \leq \mathrm{B}_{Lj}] = F(\mathrm{B}_{Lj})$

(2) $\Pr(yes - no) = \Pr[\mathrm{WTA}_j \leq \mathrm{B}_{1j} \text{ and } \mathrm{WTA}_j > \mathrm{B}_{Lj}] = F(\mathrm{B}_{1j}) - F(\mathrm{B}_{Lj})$

(3) $\Pr(no - yes) = \Pr[\mathrm{WTA}_j > \mathrm{B}_{1j} \text{ and } \mathrm{WTA}_j \leq \mathrm{B}_{Hj}] = F(\mathrm{B}_{Hj}) - F(\mathrm{B}_{1j})$

(4) $\Pr(no - no) = \Pr[\mathrm{WTA}_j > \mathrm{B}_{1j} \text{ and } \mathrm{WTA}_j > \mathrm{B}_{Hj}] = 1 - F(\mathrm{B}_{Hj})$

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:

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

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 vector x_j is 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 $E(\mathrm{WTA}) = \bar{x}\beta$ 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 (t_j) were in the \$10 ~ \$200 range as follows: (\$20, \$10, \$40), (\$40, \$20, \$80), (\$60, \$30, \$120), (\$80, \$40, \$160) and (\$100, \$50, \$200), where each number represents (first bid B_1, subsequent lower bid B_L, subsequent higher bid B_H). 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, more specific questions were presented. WTA is often impacted by individual attitudes and demographic characteristics. WTA survey collected several covariates for later incorporation into the model. Demographic information (including gender, age, education, and monthly expenditure) and the usage time on SNS (like use duration at a time, use frequency a day, and use period) was collected. Privacy invasion experience, the level of own information open, and use ability on SNS were checked by a five-point scale item. It is also conducted to other measures of event participation number and follower number.

These processes require respondents to evaluate relative to information privacy that exist on SNS. This survey was conducted through online. It was 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 research are presented in Table 2. It reports the estimated mean WTA values for each of the 13 conditions. This left us with a final sample of 293 respondents.

Table 2: Descriptive Statistics

Variable	Section	Statistics	Total	Standard deviation	Mean
WTA (DBDC)	No-No = 1	104	293	1.31	2.59
	No-Yes = 2	22			
	Yes-No = 3	57			
	Yes-Yes = 4	110			
Bid	$20:	56	293	$28.35	$60.75
	$40	59			
	$60	57			
	$80	60			
	$100	61			
Gender	Male = 1	149	293	0.5	0.51
	Female = 0	144			
Education	High = 1	182	293	0.95	3.47
	Low = 0	111			
Age	Twenties	60	293	10.61	38.88
	Thirties	94			
	Forties	73.			
	Fifties	66			
The number of event participation	Yea = 1	174	293	1.2	2.15
	No = 0	119			
The number of followers	less than 20	52	293	1.3	2.85
	20 ~ 50	76			
	50 ~ 100	69			
	100 ~ 200	57			
	more than 100	39			
Monthly expenditure	$100 ~ $700	293	293	$1266	$1561
Frequency of daily SNS use	1 and less	78	293	1.22	2.35
	2~5 times	112			
	6~10 times	51			
	11~20 times	25			
	more than 21 times	27			
Duration of SNS use at a time	10 min. and less	97	293	1.1	2.14
	10~30 min.	109			
	30~60 min.	50			
	1~2 hour	24			
	more than 2 hour	13			
Tenure of SNS use	1 year and less	43	293	1.22	3.05
	1~2 years	64			
	2~3 years	81			
	3~4 years	46			
	more than 4 years	59			
Privacy invasion experience	No = 0	155	293	0.5	0.47
	Yes = 1	138			

Results

This study investigated the WTA value of information privacy on SNS through 13 conditions about the features of SNS users. Firstly, in demographic variables Education shows 1% significance level and B value of -0.217. Age shows 5% significance level and B value of 0.139. That is, the higher is education or the younger is age, the higher is WTA. These explain that younger people with higher levels of education are more sensitive to information privacy on SNS. While, Monthly expenditure shows 10% significance level and B value of 0.003. The square of Monthly expenditure shows 5% significance level and B value of -8.724e-6. Generally, the more is Monthly expenditure, the lower is WTA. However, WTA after a certain expenditure is the higher. These explain that those spend more money monthly are less sensitive to information privacy on SNS. However, if Monthly expenditure is the far more, they are more sensitive to information privacy on SNS. Gender of demographic variables is not significant in statistics.

In the characteristic variables of SNS users, SNS use ability shows 5% significance level and B value of 0.208. That is, the higher is SNS use ability, the lower is WTA. This explains those with higher SNS use ability are less sensitive to information privacy on SNS because users tend to have lower privacy concerns if they perceive a certain degree of control over the collection and use of their personal information (Nowak & Phelps 1997; Sheehan & Hoy 2000). The number of followers shows 5% significance level and B value of -0.159. That is, the more is the number of followers, the higher is WTA. This explains those with more followers are more sensitive to information privacy on SNS. In contrast, the number of event participation shows 5% significance level and B value of 0.161. That is, the more is event participation, the lower is WTA. This explains that those with more event participation experience are less sensitive to information privacy on SNS. According to the argument of Bates (1964), personal experiences guide behavior in activities that can be subjectively deemed as privacy-related. Personal experiences like event participation experience cause a change in privacy concern over an individual's lifetime (Harris 1991). Therefore, those with more event participation experience may be lower information privacy concern. Table 3 shows the ordered logistic regression results of WTA from the features of SNS users.

Table 3. Ordered Logistic Regression Result

Variable	B	S.E,	Wald	P-value
Bid	6.228e-6	2.703e-6	5.308	***0.021*** **
Gender	-0.066	0.160	0.167	0.682
Education	-0.217	0.084	6.706	***0.010*** ***
Age	0.139	0.062	5.024	***0.025*** **
Monthly expenditure	0.003	0.002	2.755	***0.097*** *
Monthly expenditure^2	-8.724e-6	3.944e-6	4.892	***0.027*** **
SNS use ability	0.208	0.098	4.531	***0.033*** **
The number of followers	-0.159	0.069	5.376	***0.020*** **
The number of event participation	0.161	0.069	5.445	***0.020*** **
Frequency of daily SNS use	-0.018	0.092	0.036	0.849
Duration of SNS use at a time	-0.080	0.094	0.724	0.395
Tenure of SNS use	0.155	0.064	5.921	***0.015*** **
Account open limit	-0.337	0.100	11.263	***0.001*** ***
Privacy invasion experience	-0.389	0.165	5.557	***0.018*** **
Constant	-1.165	0.642	3.288	***0.070*** *
-2 Log Likelihood: 676.944, Cox & Snell R^2: 0.170, Nagelkerke R^2: 0.185				

*Significant at 1%***, 5%**, and 10%* respectively*

In SNS usage cycle variables, Tenure of SNS use shows 5% significance level and B value of 0.155. That is, the shorter is SNS use period, the higher is WTA. This explains that those who have long-time experience on SNS are less sensitive to information privacy. However, frequency of daily SNS use and duration of SNS use at a time are not significant in statistics. To result, according to the argument of

Westin (1967) that privacy is the ability of the individual to control the terms under which personal information is acquired and used those with longer Tenure of SNS Use should have lower information privacy concern because they have disclosed their information on SNS for a long time

In the privacy related variables on SNS, Account open limit shows 1% significance level and B value of -0.337. That is, the higher is Account open limit, the higher is WTA. This explains that those limit account open are more sensitive to information privacy on SNS. While, Privacy invasion experience shows 5% significance level and B value of -0.389. That is, if there is Privacy invasion experience, WTA is the higher. This explains that those with privacy invasion experience are more sensitive to information privacy on SNS. Previous privacy invasion experience could affect an individual's concern for privacy (Culnan 1993). According to the argument of Awad & Krishnan (2006), for example, those with previous privacy invasion experience have a lower willingness to be profiled online for personalized advertising. Therefore, they may be higher information privacy concern.

Table 4. WTA value for information privacy on SNS

Section	Sub Section	WTA value ($)	Observations
TOTAL		$28	293
Gender	Female	$530	144
	Male	$4	149
Education	Low	$23	111
	High	$170	182
Age	20	$0	60
	30	$72	94
	40	$0	73
	50	-$41	66
Job	Employee	$11	178
	Unemployee	-$6	115
Monthly expenditure	less than $200	$51	187
	more than $200	$9	106
SNS firms	Facebook	$23	202
	Twitter	$0	44
	KakaO	$98	211
	Band	$12	66
	SNS_O	$47	62
SNS Type	Private	$81	246
	open	$44	229
The type of SNS information	Friend	$252	130
	Profile	$494	170
	Location	$406	78
	Life	$140	56
	Inference	$0	69
	Chat	$0	45
	Information_O	$0	38
The purpose of SNS use	Friendship	$70	249
	Sharing	$1	98
	Collecting	$5	100
	Self	$66	99
	Purpose_O	$77	38

The next step for evaluating the value of WTA is to compute the average of 13 conditions on the monetary value of information privacy on SNS. Table 4 shows the WTA value of information privacy on SNS. The total WTA value mean of users is $28/number. In detail, the WTA value of female is $530/number, but that of male is $4/number. This means that the information privacy value of female on SNS is much higher than that of male. The WTA value of low education users is $23/number, but that of high education users is $170/number. This means that the information privacy value of high education users on SNS is higher than that of low education users. In Age, also, the WTA value of 30

age is only $72. The WTA value of rest age is zero or minus. In demographic variable, therefore, the high educated female in their 30s praise highly the monetary value of information privacy on SNS.

The WTA value of employee users is $11/number, but that of unemployee users is minus. This means that the information privacy value of employee users on SNS is higher than that of unemployee users. However, both are lower than total WTA value and make only a few odds. This shows that it can be not important whether SNS users are employee or not. Whereas, the WTA value of those that spend less than $200 monthly is $51/number, but that of those that spend more than $200 monthly is $9/number. This means that frugal users praise highly the monetary value of information privacy than prodigal one. To result, these explain that the consumption of users is more important than the income of users in the WTA value gap of information privacy on SNS.

Table 5. Summary of WTA results of information privacy on SNS

Section	The summary of WTA results in higher WTA
Demographic	(in higher WTA) - The higher education - The younger age - The less Monthly Expenditure or The far more Monthly Expenditure The high educated female in their 30s praise highly the monetary value of information privacy on SNS. The consumption of users is more important than the income of users in the WTA value gap of information privacy on SNS.
Characteristic of SNS users	(in higher WTA) - The lower SNS use ability - The more number of followers - The little event experiences
SNS usage cycle	(in higher WTA) - The shorter SNS use period
Privacy related	(in higher WTA) - The higher Account Open Limit level - If there was Privacy Invasion experiences
Type of SNS	The monetary value of information privacy on private SNS like Kakao-Talk and Band is higher than that on open-SNS like Facebook and Twitter. The users' WTA value of Kakao-Talk of SNSs is the most expensive at $98/number.
Type of SNS information.	The value of Profile and Location information is higher than any other SNS information.
Purpose of SNS	The value of Friendship and Self purposes is higher than any other SNS purpose.

Demographic, SNS users' characteristics, SNS usage cycle, and Privacy are 'Ordered Logistics Regression Result' of Table 3.
Type of SNS, Type of SNS information, and Purpose of SNS are 'WTA estimation for information privacy on SNS' of Table 4

In type of SNS, the WTA value of private SNS users is $81/number, but that of open-SNS users is $44/number. This means that the monetary value of information privacy on private SNS is higher than that on open-SNS. In detail, the monetary value of information privacy per SNS firms is evaluated. The users' WTA value of Kakao-Talk and Band as private SNS is each $98/number and $12/number, but that of Facebook and Twitter as open-SNS users is each $23/number and zero.

In the type of SNS information, each WTA mean of Friend, Profile, Location and Life information is $252/number, $494/number, $406/number and $140/number. The others like Inference and Chat are worthless. This shows that SNS users praise highly the value of Profile and Location information. According to the argument of Acquisti & Gross (2006), those with profiles on SNS had greater concerns than those who did not have profiles. The concerns of location information pertain to the accumulated customer information and the potential risk that consumers would experience with a breach of confidentiality (Gidari 2000). Continuous location information often reveals the position of a person in real time (Beinat 2001). Such a collection of information is subject to potential abuse and improper handling of such information can expose customers to significant risk. Therefore, Profile and Location information have the highest value of SNS information.

In the use purpose of SNS, each WTA mean of Friendship, Sharing, Collecting and Self is $70/number, $1/number, $5/number, and $66/number. This explains that those with more individual purpose like Friendship and Self should have the higher monetary value of information privacy because they have already known the importance of information privacy. Table 5 shows the summary of results estimating the WTA value of information privacy on SNS.

Discussion

This paper investigated the monetary value of information privacy on SNS through 13 conditions (about the demographic variables, the characteristic of SNS users, and SNS features). As a result, sensitive SNS users for information privacy have following characteristics: 30s, higher education, the less Monthly Expenditure or the far more monthly expenditure, lower SNS use ability, more number of followers, little event experiences, shorter SNS experience, higher account open limit level and privacy invasion experiences.

Especially, younger people are more sensitive to information privacy on SNS. However, the 20's monetary value of information privacy on SNS is zero. It is much easier to become a 'friend' online than offline and many users do not restrict their privacy settings to only friends. Younger people are more willing to place personal information on their profiles as they believe, and assume that most people who view their page will be 'friends'. However, these privacy concerns are further compounded by the new instant 'chat' feature where more personal conversations can take place with 'friends.' Personal information on SNS is also being volunteered because of changing cultural trends, increased familiarity and confidence in technology. Information on profile pages is a particularly difficult area, as users are volunteering information which they have a right to do. Many young people are simply not aware of what may happen to the information they place on these profiles. Although a SNS user offers 'consent' when they sign up to an online site, most are unaware of the implications of voluntarily providing personal information on profiles as well as not being aware of how this information may be processed. An individual can lose control of their data when a digital dossier of personal information is generated. This occurs when profiles on SNS can be downloaded and stored over time by site operators for back up purposes so as to incrementally create a digital dossier of personal information. This can also occur out of the control of the user as users' 'friends' on their sites can write a comment about them on another friends' profile or 'tag' the individual in photos. It is in this way that profile information has the potential to be used in ways that the user did not intend and stored for indefinite periods. The main threat associated with digital dossier aggregation for young users is when future employees or colleges are able to perform searches that may bring up data or even compromising photos that an individual thought either no longer existed or not possible for that source to obtain. Therefore, the 20's monetary value of information privacy on SNS can be the lower than the 30's one.

Also, gender is not significant in statistics. In a meta-analysis of 150 studies of different age groups published from 1964 to 1997, most of the studies provide evidence for greater risk taking among men than women (Pompili et al. 2007). These results may not be singularity in information privacy on SNS.

The average of 13 conditions on the monetary value of information privacy on SNS was computed. The total WTA mean is $28/number (Table 4 references). The monetary value of information privacy according to SNS features have the following characteristics. First, those who use private SNS like Kakao-Talk and Band have the more sensitive of information privacy. The monetary value of information privacy on private SNS is thus higher than that on open SNS like Facebook and Twitter. In detail, the users' WTA value of Kakao-Talk and Band as private SNS is each $98/number and $12/number, but that of Facebook and Twitter as open-SNS users is each $23/number and zero. Using these mean WTA, information privacy value of all users for each SNS firms can also be estimated. Considering that there are about 20 million users (Kakao-Story), 15 million users (Band) and 10 million users (Facebook) in Korea[1], the estimated monetary value of information privacy for each Facebook, Twitter, Kakao-Story, and Band would be about $230 million, $0, $1,960 million, and $180 million. In other word, SNS firms own the $180 ~$1960 worth of information privacy, except twitter. By computing the monetary value of information privacy on SNS, second, this research found that the value of Profile and Location information is relatively more important than others. Third, by considering the purpose of SNS use, it found that Sharing and Friendship purpose are more important than other purposes in terms of information privacy. These results are consistent with idea of Boyd & Ellison (2007) that emphasizes 'friends' and 'profiles' as the most basic information. These can explain that those with more friendship, relationship, and sociality and higher pride that can expose confidently own information on SNS profiles have the higher monetary value of information privacy.

This paper has several implications for research. First, it tried to figure out the various factors that affect the monetary value of information privacy on SNS. Here, it is found that longer, various, and more 'experience' for Time and SNS use in relation to SNS can have an impact on the monetary value of information privacy. Therefore, the results of this paper can help SNS users figure out the factors that affect the monetary value of information privacy and how important they perceive the information privacy of themselves on SNS.

Regarding managerial implications, second, it is worthy of notice for practitioners that provide and operate SNS or managers who want to use SNS as a marketing channel. Recently, the reason that private SNS such as Kakao-Talk and Band grow rapidly might be due to increasing privacy concerns on open-SNS. As online SNS market has rapidly grown, the SNS user preference has shifted from open SNS to private SNS which provides closer, more private space; it reflects the issues with open SNS such as invasion of privacy and flood of advertising. As a result, the age group of private SNS users has expanded to those in their 50s and above, forming a network with real-names and social relationships on a daily basis. Also, the private SNS has led to increased offline interactions and is being used actively. In particular, 'BAND' in Korea has established itself as a top, sustainable private SNS, as it allows users in their 40s and above to easily build their own network with friends and family members online. In the result of this paper, the monetary value of information privacy on private SNS is higher. After all, it implies that the protection of information privacy on SNS can be actively managing or increasing the value of them. Most of previous researches do not suggest an enough explanation on the protection of information privacy, but it can lead to improve the privacy protection strategy of SNS firms. In detail, this paper provides results that SNS marketers can utilize to encourage customer participation in online profiling for personalized service and advertising. SNS marketers must realize that the perceived value provided to customers can affect the degree to which their previous privacy issues come to bear. SNS firms must provide a benefit to offset the potential risk to customers for sharing their information with the firm.

Third, combining privacy literatures in information system researches together with CVM in economics, it extended the horizon of privacy studies one step further. It conducted this approach because there

[1] by Nielsen Korea (http://www.etnews.com/20151228000205)

has 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. It made the results on the monetary value of information privacy on SNS more persuasive by analyzing an ordered logistic regression model.

To one's regret, SNSs of this study are limited to popular ones in Korea. In order to draw global and general conclusions, we are collecting additional data in US. In future research, we expect more improved results and new implications.

References

Aïmeur, E., G. Brassard, and F. S. M. Onana. Privacy-preserving demographic filtering. in Proceedings of the 2006 ACM symposium on Applied computing. 2006. Dijon, pp. 872 - 878.

Awad, N. F. and M. S. Krishnan "The Personalization Privacy Paradox", MIS Quarterly Vol. 30 No. 1, pp. 13-28/March 2006

Bauer, Talya N., Donald M. Truxillo, Jennifer S. Tucker, Vaunne Weathers, Marilena Bertolino, Berrin Erdogan, and Michael A. Campion "Selection in the Information Age: The Impact of Privacy Concerns and Computer Experience on Applicant Reactions", *Journal of Management*, Vol. 32 No. 5, October 2006 601-621

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: a review of information privacy research in information systems," *MIS quarterly* (25:4), pp. 1017-1042.

Bomil, S.: An Exploratory Study on the Characteristics of Online Social Network and Purpose of Custimer's Use. Journal of Information Technology Applications & Management (2013)

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

Boyd, D. M., and Ellison, N. B. 2007. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13:1), pp. 210-230.

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

Culnan, M.J., and Armstrong, P.K. 1999. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science* (10:1), pp 104–115.

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), pp. 57-93.

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

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), pp. 13-42.

Hanemann, W. M. 1984. "Welfare Evaluation in Contingent Valuation Experiments with Discrete Responses," *American Journal of Agricultural Economics* (66:3), pp. 332-341.

Hanemann, W. M. 1994. "Valuing the Environment through Contingent Valuation," *Journal of Economic Perspectives* (8:4), pp. 19-43.

Hausman, J. A. 1993. Contingent Valuation: A critical Assessment, Amsterdam, North Holland Press

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.

Jinhyeong, L.: Diffusion and Trends of SNS. Jounal of Communication & Radio Specetrun (2012)

Kim, Cheongah and Younghwan Pan "A Study on Private SNS (Social Networking Service) Usage of Seniors" C. Stephanidis (Ed.): HCII 2014 Posters, Part II, CCIS 435, pp. 37–42, 2014.

Lohr, S. 2010 "http://www.nytimes.com/2010/03/17/technology/17privacy.html," 'How privacy vanishes online', March 16.

Mackaay, E., 1990. "Economic Incentives in Markets for Information and Innovation," *Harvard Journal of Law & Public Policy* (13:3), pp. 867-910.

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), pp. 336-355.

Margulis, Stephen T. "Privacy as a Social Issue and Behavioral Concept" *Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 243—261*

McLean, I., & McMillan, A. 2009 “Conservatism, Concise Oxford Dictionary of Politics, Third Edition, sometimes it (conservatism) has been outright opposition, based on an existing model of society that is considered right for all time. It can take a 'reactionary' form, harking back to, and attempting to reconstruct, forms of society which existed in an earlier period,” Oxford University Press.

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

Mundy, B., and McLean, D. 1998. “Using the Contingent Value Approach for Natural Resource and Environmental Damage Applications,” *The Appraisal Journal* (66), pp. 290-297.

Raghu, T. S., Sinha, R., Vinze, A., and Burton, O. 2009. “Willingness to Pay in an Open Source Software Environment," *Information Systems Research* (20:2), pp. 218-236.

Rosenblum, D. 2007. "What Anyone Can Know: The Privacy Risks of Social Networking Sites," *Security & Privacy, Volume* (5:3), pp. 40-49.

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*, A. Hozinger, M. Ziefle, M. Hitz and M. Debevc (eds.) Heidelberg: Springer Berlin Heidelberg, pp. 174-193.

Skinner, G., Han, S., and Chang, E. 2006. “An Information Privacy Taxonomy for Collaborative Environments,” *Information Management & Computer Security* (14:4), pp. 382-394.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. “Information Privacy: Measuring Individuals' Concerns about Organizational Practices,” *MIS Quarterly* (20:2), pp. 167-196.

Smith, H. Jeff, Dinev, Tamara, and Xu, Heng, 2011 Information privacy research: an interdisciplinary review, MIS Quarterly, v.35 n.4, p.989-1016, December 2011

Solove, D. J. 2006. “A Taxonomy of Privacy,” *University of Pennsylvania Law Review* (154:3), pp. 477-564.

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

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

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), pp. 415-444.

Wallbridge R. 2009. “How Safe is Your Facebook Profile? Privacy Issues of Online Social Networks,” *ANU Undergraduate Research Journal* (1), pp. 85-92.

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

Wieschowski, S. (2007). Studenten demonstrieren gegen das Schnu¨ffelVZ, [www document] http://www.spiegel.de/netzwelt/web/0,1518,523906,00.html (accessed 28th October 2009).