Asia Pacific Journal of Information Systems
Vol. 28 No. 3 (September 2018), 154-166

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2018.28.3.154

The Value of Personal Information: An Exploratory Study for Types of Personal Information and Its Value

Minjung Park[a], Sangmi Chai[b,*]

[a] *Ph.D. candidate, School of Business, Ewha Womans University, Korea*
[b] *Associate Professor, School of Business, Ewha Womans University, Korea*

ABSTRACT

As the number of online privacy incidents are increasing, lawsuits related with personal information infringements have been also growing as well. However, there are large differences between a plaintiff and a defendant to determine the amount of payment for damages from the incident. After the verdict was made, a plaintiff is not satisfied with the amount of compensation, whereas a defendant usually tries to their best to reduce the payment amount. This is because the value for personal information are hardly assessed exactly. In addition, there is no criteria for calculating the price of the information itself. Since the development of information technology enables the firms could collect and use any piece of information to identify a particular individual, the range of personal information has been also broadening. Based on these phenomenon, this study tries to grouping the types of personal information and exploring the perceived value of types of information. Therefore, this study could provide a foundation for narrowing the gap of the value of personal information between the firm and the defendant. Through AHP (Analytic Hierarchy Process), this study finds out that people usually value more on biometrics information, medical records, and criminal records whereas weigh less for email address and date of birth.

Keywords: AHP (Analytic Hierarchy Process), Personal Information, Personal Information Value, Priority of Personal Information

Ⅰ. Introduction

In 2014, over 100 million clients' personal data, including bank account numbers and credit ratings, was leaked from a major credit card companies in Korea, KB Card Co., NH Card Co. and Lotte Card Co. A local court sentenced three credit card companies to compensate about eighty dollars to each victim (Ham and Park, 2017). Although the judgment clearly confirmed that the liable party was the credit card

*Corresponding Author. E-mail: smchai@ewha.ac.kr Tel: 82232772780

companies because they had not complied with the privacy protection law and failed to fulfilled proper supervision duty for their employees in keeping customers' personal information, the amount of compensation made from the judgment was controversial (Chosunbiz, 2018.02.17). There were strong opinions that 80 dollars of compensation for each victim is a way below amount compared with the case made in other advanced countries in online privacy protection like US. If we take a deep look in the sentence made, the court determined the amount of compensation based on the fact that the card holders' social security number was leaked or not. The judgment implies that social security number has different value, compared to other personal information, such as e-mail, name or phone number leaked as well. Therefore, we can assume that the Korean court recognized the different value of each types of personal information. However, the amount of financial compensation is usually determined uniformly, irrespective of the types and the amount of personal information leaked. As a result, there could be a dispute between a victim who has infringed his or her personal information and the company which accompanied with liability regarding the amount of compensations. Consequently, the companies and clients could not reach to agreement with the regal decision so that they decided to continue further civil or criminal lawsuits (Yonhapnews, 2016.07.28).

As the number of personal information breaches has risen steeply, people are getting to recognize the perceived importance of personal information more compared with the past time. According to a survey, about 52% of the respondents said that it would be appropriate to estimate the amount of compensation per person is more than thousand dollars when personal information is leaked (Security News, 2016.08.01). The result of the survey shows that a value of personal information perceived by individuals is considerably higher than eighty dollars which is an amount from the verdict made by the Korean court after the three credit card companies' personal information breach incidents. It is expected to be increased in the future that a gap of value between the victim and the company regarding personal information when the breach incident happens. Based on these phenomenon, we assume that the perceived value of personal information is vary by each individual and types of information. Therefore, in this study, we assume that people would value differently for their personal information and there would be some common criteria to group personal information such as biometric information, financial records and medical history etc. This study adopted AHP, which is a useful method to derive a priority by comparing various subjective items, to identify value order for personal information.

The results of this study can provide the useful criteria for evaluating appropriate amount of compensations when personal information breaches occur. In addition, it also contributes to reduce unnecessary cost for extra litigations arise from a disagreement on a compensation amount. Furthermore, our study results could be utilized for firms and governments to establish their policy or law for collecting, processing, and storing customers' personal information throughout information systems.

Ⅱ. Literature Review

2.1. Type of Personal Information

Personal information is defined as a collection of data that can be explained the particular individual's identity such as names, addresses, lifestyle

interests, shopping preferences, and purchase histories of identifiable individuals (Nowak and Phelps, 1995). As various kind of user authentication methods for using IT devices and other online services like online banking and mobile payments are becoming more widespread, a lot of criminal activities that have intentions to steal personal information are also increasing as well (Simoens et al., 2012). By using personally identifiable information (PII), which is a main target of personal information infringements crime, the third party can easily identify a particular individual. In other words, using PII by a third party without owners' consents can lead to crimes such as illegal credit card payments and cash withdrawal. PII is any data that can be used to identify a specific individual, such as phone number, date of birth, social security number and behavioral information of a person (Tasidou et al., 2009). In addition, geolocation information, biometric data, IP addresses, login IDs, social media posts, or digital images can also be classified into PII (McCallister et al., 2010). Therefore, it can be defined as information which can be used to trace or distinguish an individual's identity either alone or when combined with other personal information that is linkable to a specific individual (Krishnamurthy and Wills, 2009).

Users have begun to recognize the value of PII more importantly than any other personal information these days since there are growing number of services including financial services provided online based on user authentications. As a consequence, their protection intentions for PII have also increased. Phelps et al. (2000) examined how users' intentions to provide personal information differ according to a type of personal information. The results showed that participants showed the highest intention to share demographic information (e.g., age and occupation) among other types of personal information. However, they had moderate intention to provide purchase-related information and the least intention to provide PII such as telephone number, social security number and kinds of credit cards they owned. People also have a tendency to consider medical and financial data is highly sensitive data while their gender, age or nationality are considered less sensitive one (Cranor et al., 2000). Prior study provided evidential research results supporting our study assumption that users' perceived importance for each type of personal information could be varied by types.

There has been an attempt to classify and categorize various types of personal information. Each country has different definitions about what is PII and classify them in accordance with their sensitivity and vulnerabilities (Janczewski and Shi, 2002). Although there are legal definitions of what personal data and PII is, and regulations are provided for how they should be collected and processed by law for each government (e.g., in the General Data Protection Regulation of the EU and in US privacy law), people usually perceive the value of their personal information differently depending on their situations and personal characteristics (Van Zoonen, 2016). Thus, we aim to derive the amount of different value for each types of personal information in PII based on assessments of people's perceived importance for each category in PII.

2.2. Perceived Value of Personal Information

The value of personal information can be defined by in a perspective of economic, social and personal value. First, personal information has social value as it should be protected and managed by law (Yoo et al., 2009). The value of personal information is also evaluated as the intention of a customer to provide personal information in the market, in an eco-

nomic perspective (Montes et al., 2015). Individuals perceive value of personal information when they can achieve expected satisfactions by acquiring specific services or products through providing personal information (Kashyap and Bojanic, 2000).

Individuals' perceived value of personal information is changing by personal traits and contextual factors (Yu et al., 2010). Park et al. (2017) investigated the value of personal information. According to their results, an individual's perceived value of personal information is influenced by individuals' risk aversion and situational properties by adopting cost-benefit analysis framework. The results of the study showed, as the individuals' perceived risk increases, the value of personal information increases as well. Users who are using open-based SNS tend to perceive low economic value of personal information in compared to those who are using close-based SNS due to their personal dispositions as openness (Jung and Lee, 2015). Individuals' perceived value of personal information affects an individual's information security behaviors. Park et al. (2014) identified that the users' perceived value in the use of location-based services enhances the intention of information security behaviors. Acquisti (2004), on the other hand, presented, privacy paradox, that individuals' perceived value, based on threats, did not always increase the intentions of information protection behaviors. Therefore, we can infer individuals' perceived value of personal information dose not generate consistent privacy protective behaviors.

As we above mentioned, personal information has a trouble for establishing a fixed economic value because it is an intangible asset that can be changed by its given situations or subjects' characteristics. Additionally, it does not produce consistent individuals' behaviors related on personal information protection behaviors. Therefore, when a personal information invasion occurs, a victim has a difficulty to prove the exact amount of his or her damage from the incident. A company, which has a liability for personal information invasion, is also hard to compensate the correct amount of damage. Thus, it is necessary to identify the individuals' priority of personal information. Deriving priority of individuals' perceived value of personal information will contribute to the establishment of a basis for calculating appropriate amount of compensation, in the future. Firms also can forecast customers' personal information behaviors based on their priority of personal information. In this study, we derive the estimated the value of the type of personal information using AHP, which is suitable for identifying the priority.

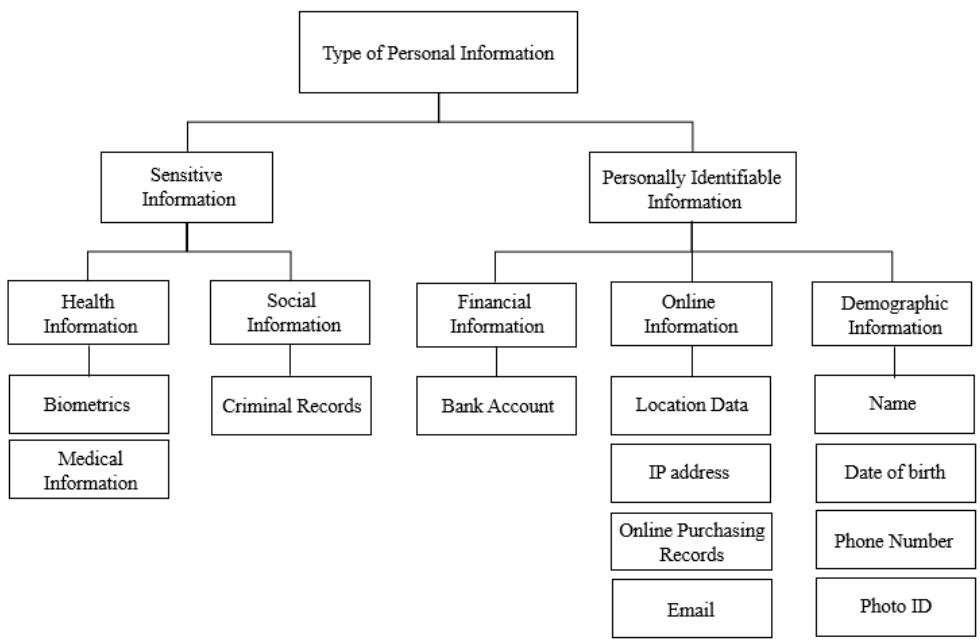
Ⅲ. AHP Model

We constructed a hierarchical model for figuring out the individuals' perceived value order of personal information. We divided sensitive information and PII at first level in AHP model. According to article 23 and 24 of Privacy Act, in Korea, it regulates PII and sensitive information should be processed differently. It assumes that whole personal information consists of PII and sensitive information. Furthermore, GDPR(General Data Protection Regulation) also classifies personal information into PII and sensitive information and it holds sensitive information will be required more stringent security, since the impact of dissemination is considered more egregious Schoch, T. P. (2016). Based on it, a few studies adopted this classification of personal information and identified how this type of PII and sensitive information have to be controlled effectively, in a firm's perceptive

(Terzi et al., 2015), at the same time, the others investigates users' how perceive or disclose their personal information differently, according to its type of it in online (Bansal and Gefen, 2016; Liu and Lwin, 2016). Therefore, we applied same classification of personal information.

We mainly adopted the type of personal information classified by Korea Internet Security Agency(KISA) and modified with related reports (Enterprivacy Consulting Group, 2017; PrivacySense.net, 2018). They suggest personal information consist of next major category: finance, physical, social, online communication and basic information. Based on this criteria, we construct AHP model as shown in <Figure 1>.

Health information which includes biometrics (e.g., DNA code, iris and fingerprints) and medical information are classified as sensitive information. Medical information describes an individual's medical conditions or physical and mental health, drug test results, disabilities, family or individual health history, blood type, prescriptions and health records. Sensitive information also includes information about an individual's criminal activity such as convictions, charges and legal responsibilities. We use criminal records for identifying how users' perceived value of social information is different, even though social information includes military service information and labor information, as well. The participants we target in this study, they have no duty for military service and do not employed in workplace. Therefore, we choose only the most common social information as criminal records, except for military service and labor information. In this study, we classified PII into financial, online behavioral and demographic information. Financial information that identifies an individual's financial account and behavioral information that describes an individual's on-line overall behaviors or activities. For example, purchase recodes via online store, email,



<Figure 1> AHP Model

IP address and location data which can be collected by GPS. Demographic information that describes an individual's characteristics such as name, date of birth, phone number and photo ID.

Ⅳ. Research Design

4.1. AHP (Analytic Hierarchy Process)

In this study, AHP (Analytic Hierarchy Process) methodology was applied in order to figure out individuals' perceived value priority of type of personal information. AHP is a multi-criteria decision-making method that is used in situations where uncertain situations or various evaluation criteria are needed (Byun, 1999; Saaty, 1977). In other words, it is usually used for treating complex decision making, and may support the decision maker to set priorities and make the best decision (Lipovetsky and Conklin, 2015). It assumes humans' inconsistency in judgment because they cannot be always consistent (Ishizaka and Lusti, 2006; Saaty, 1977). Therefore, AHP is an effective way when propose a policy by utilizing pairwise comparisons between the variables and quantifying participants' subjective decisions (Ko and Ha, 2008). By reducing complicate decisions to a series of pairwise comparisons, and then synthesizing the results, the AHP helps to capture both subjective and objective aspects of a decision (Dyer and Forman, 1992). The ratio scales are derived from the principal Eigen vectors and the consistency index(CI) is derived from the principal Eigen value (Ramanathan and Ganesh, 1994; Saaty, 1994; Saaty, 2003). CI is a measure of consistency, AHP calculates a consistency ratio (CR) comparing CI of the matrix in question versus the consistency index of a random-like matrix (RI). CR is generally accepted when its value is smaller or equal to 0.1 (10%), but less than 0.2 (20%) is also considered suitable for analysis. (Wind and Saaty, 1980).

4.2. Data Collection & Process

We investigated total of 44 participants for identifying the value priority of personal information that people perceived. We carry out in-death paper-based survey of AHP model applying for females whose age is range from 20 to 27. We targeted for participants who took at least one requisite course related to information security in university for ensuring their expertise of information security. Individuals' perceptions of information security are influenced with gender, age and education. Xie and Kang (2015) identified that male and older users are more likely to disclose their personal information in SNS because while the younger and female users are more perceived privacy risks. Additionally, males are more likely to engage in downloading and purchasing activities while females are more likely to engage in messaging activities, depended by difference of their perceived security in online (Teo, 2001). These results show that gender and age impact to users' overall perceptions and behaviors of information security. Based on prior findings, we need to manipulate the demographics of participants, Therefore, we target for only female students, who belong to similar age groups and have an experience of taking a lecture of information security in university, to control participants' personality, cultural background and awareness of information security.

The main purpose of the survey to figure out the rank of importance of each categories of personal information. 12 types of personal information, as described in <Figure 1>, were used to establish the pairwise comparison matrix and some items were

<Table 1> AHP Questionnaire

Factor	← More important than				Equal	Less important than →				Factor
	5	4	3	2	1	2	3	4	5	
Name										Date of birth
Name										IP address
Name										Email
Name										Criminal Records

provided with definitions and examples to help participants' understanding. For example, biometric information, which may be a relatively new concept for participants, was presented with definitions and examples such as fingerprints, iris and genetic information. AHP allows individuals to choose a value between 1 to 9 with which to rate the strength of the relationship between items in order to establish the pairwise comparison matrix so as to calculate the related eigenvalues and the eigenvectors (Chiu et al., 2010). Finally, a questionnaire consisting of all category of personal information criteria and subcriteria of the two levels of the AHP model was designed and was used to collect the pairwise comparison judgments. The following <Table 1>. shows some of the items of the AHP we conducted.

To resolve the consistency problem that appears in pairwise comparisons, the verification of CR was conducted during the AHP analysis. The responses were excluded when CR goes beyond 0.2, finally, 39 of them were used. The analysis for this research was conducted in DRESS 1.5 program. We used geometric mean for identifying each of the weighted value of personal information.

Ⅴ. Results of AHP Analysis

After analyzing the priority of personal information by AHP, the weighted value of biometrics was the highest at 0.169 which means the participants in this study regarded biometrics as the most important personal information in compared to the others. The weighted value of medical information was ranked as second with 0.137 value, and the weighted value of data of birth was the lowest at 0.030. This result indicates that components of health information (i.e., biometrics and medical information) had the highest relative importance among 12 types of personal information. The weighted value for criminal recodes was appeared as the third importance with 0.108. We can conclude sensitive information which include health and social information were regarded as more important than PII. Therefore, it can be explained that it is reasonable for sensitive information to be more strictly protected than the other personal information by law. Most of countries regulate that sensitive information should be treated with extra caution because its impacts of damages caused by the breaches or leakage are very serious. Data processing of sensitive information is also prohibited unless it is an exceptional case permitted by law. Among online behavioral information, users responded on the relative importance in the order of location data, IP address, purchased records and email. We could inference that users now have begun to recognize the possibility of re-identification of themselves through a combin ation of data stored online, such as IP address and location data. Therefore, in addition to information

<Table 2> Results

Depth 1	Depth 2	Components	Weight	Rank
Sensitive Information	Health Information	Biometrics	0.169	1
		Medical Information	0.137	2
	Social Information	Criminal Records	0.108	3
Personally Identifiable Information (PII)	Financial Information	Bank Account Number	0.105	5
	Online Behavioral Information	Location data	0.084	6
		IP address	0.077	7
		Online Purchasing Records	0.048	9
		Email	0.035	11
	Demographic Information	Name	0.033	10
		Date of birth	0.030	12
		Phone Number	0.068	8
		Photo ID	0.106	4
Total			1.000	

that can identify an individual instantly such as Photo ID or name, information like online purchasing records that contain the possibility of identification through combination with other pieces of data could increase relative importance of the personal information. <Table 2>. shows the detailed result of AHP analysis.

Ⅵ. Discussions

It is necessary to assess the relative importance of types of personal information since there are growing numbers of personal information infringement accidents. Until now, there are few studies have examined the value of personal information so that is is very difficult to assess actual damages and to decide compensation amount when personal information breach accidents happen. Although prior studies tried to assess the value by using an estimation model (e.g., JNSA JO), or a contingent valuation method (CVM) (Jung and Lee, 2015; Kwon et al., 2012; Park et al., 2017; TAHAOĞLU, 2009), they overlooked that the value of personal information could be different according to its categories. Therefore, this study has an academic contribution by addressing that personal information needs to be managed by its priority and the value can be ordered based on its perceived importance. Most of societies place a biggest emphasis on the social security number among many other personal information due to the fact that it is the most usable key value to identify a particular individual for any circumstance. As bigdata analytics methods is developing quickly, any kinds of personal information can be used to identify particular individual by combined with other types of personal information, not only by social security number. Therefore, the results of this study shed light on the value of each type of personal information including social security number as accordance with fast changing IT service environments.

Prior researches in information privacy have studied personal information as a single comprehensive concept, without distinguishing the type of personal

information. They mainly have examined how users' attitudes or behaviors would be changed by their perceptions toward personal information without considering its distinctive value for each type. However, the relative importance of personal information is clearly different by its type of it, as we derive from the data analysis results. It implies the possibility for changing users' attitudes and behaviors in online privacy according to types of personal information. Many studies have found that perceived severity and risks of an individual have a significant impact on his or her personal information protection behaviors. However, if we divide the personal information into various types like biometrics and birth of date, respectively then a result would be different. Thus, the future research needs to be carried out to figure out the precedential factors affecting perceived value of types of personal information. Our study results indicate that our government and firms need to aware the different value for personal information and to reflect the differences in managing personal information.

As personal information has been transacted in the world, it is important to understand that the differences of the users' perceived value, depended by the type of personal information. Financial information has been already transacted in some of certain fields, in Korea (Hankyung, 2018.03). Therefore, we provide a foundation for estimating the price of personal information. Based on the results of this study, we can infer that it is appropriate for the biometrics should be evaluated at a higher price than e-mail address, in the market. This study also suggest that a firm should provide compensation appropriately to victims accordingly the value of infringed personal information. An incident of personal information leakage had happened in 2014, the responsible company compensated equally to the victims regardless of the type and amount of the leaked personal information. However, the results of this study suggest that victimized customers would not feel fair when the firm compensate equally regardless the type and amount of personal information breached. Therefore, our study can be used as a foundation for establishing appropriate compensation framework for personal information infringements. This study also suggest that a firm should provide compensation appropriately to victims accordingly the value of infringed personal information. An incident of personal information leakage had happened in 2014, the responsible company compensated equally to the victims regardless of the type and amount of the leaked personal information. However, the results of this study suggest that victimized customers would not feel fair when the firm compensate equally regardless the type and amount of personal information breached. Therefore, our study can be used as a foundation for establishing appropriate compensation framework for personal information infringements.

There are some limitations of this study which need to be addressed in future research. First, we extracted representative 12 items among various personal information because we could not examine the relative importance of all types of personal information. We have a plan to establish a more delicate hierarchical model by adding another personal information type such as handwriting styles, speech patterns, and gait which was not applied in this study. By constructing two levels of AHP model, in this study, we could only compare the type of personal information as in one-level, however, it needs to be established more in-depth hierarchical structure to identify more criteria of personal information value, by applying more personal information. Secondly, we focused on the overall value of personal in-

formation, although it also can be divided into social, economic and personal value. The purpose of this study is to investigate whether users perceive value can be differentiated according to the type of personal information so that we focused on its overall value. As a result, we demonstrated users' perceived value of personal information is different. Based on this result, we have a plan to conduct a future research by applying its separated value including personal, economic and social value. It will help extend the results of study and contribute to identify users' perceived value of personal information more, in detail. Third, this study investigated controlled sample respondents to answer the value by limiting gender, education, and knowledge level about cybersecurity. Users' perceptions of information security are easily influenced by many of demographic factors like their knowledge, age, cultural backgrounds, and gender so that we tried to find out only the perceived value difference on the type of personal information by controlling demographic factors of our research sample. A further study must explore demographic group differences on the perceived value of personal information.

<References>

[1] Acquisti, A. (2004). Privacy and security of personal information. *Economics of Information Security*, 179-186.

[2] Bansal, G., Zahedi, F. M., and Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

[3] Byun, D. H. (1999). AHP Model for Evaluating EIS Software Packages. *Asia Pacific Journal of Information Systems, 9*(3), 75-92.

[4] Chiu, W., Lee, Y., and Lin, T. (2010). Performance evaluation criteria for personal trainers: An analytical hierarchy process approach. *Social Behavior and Personality: An International Journal, 38*(7), 895-905.

[5] Cranor, L. F., Reagle, J., and Ackerman, M. S. (2000). Beyond concern: Understanding net users' attitudes about online privacy. *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*, 47-70.

[6] Han, J., Kang, S. B., and Moon, T. S. (2013). An empirical study on perceived value and continuous intention to use of smart phone, and the moderating effect of personal innovativeness. *Asia Pacific Journal of Information Systems, 23*(4), 53-84.

[7] Ham, S., and Park, D. (2017). Study on policies for national cybersecurity. *Journal of the Korea Institute of Information and Communication Engineering, 21*(9), 1666-1673.

[8] Ishizaka, A., and Lusti, M. (2006). How to derive priorities in AHP: A comparative study. *Central European Journal of Operations Research, 14*(4), 387-400.

[9] IGP, C., and CIPP, C. (2016). EU privacy regulations' impact on information governance. *Information Management, 50*(1), 20.

[10] Janczewski, L., and Shi, F. X. (2002). Development of information security baselines for healthcare information systems in new zealand. *Computers & Security, 21*(2), 172-192.

[11] Jung, W., and Lee, S. T. (2015). What affects the value of information privacy on SNS? *Asia Pacific Journal of Information Systems, 25*(2), 289-305.

[12] Kashyap, R., and Bojanic, D. C. (2000). A structural analysis of value, quality, and price perceptions of business and leisure travelers. *Journal of travel research, 39*(1), 45-51.

[13] Ko, K., and Ha, H. (2008). Meta analysis of the utilization of analytic hierarchy process for policy studies in korea. *Korean Policy Studies Review, 17*(1), 287-313.

[14] Krishnamurthy, B., and Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. *Proceedings of the 2nd ACM Workshop on Online Social Networks*, 7-12.

[15] Kwon, H., Lee, E., Kim, T., and Jun, H. (2012). Estimating compensation for personal information infringement in korea using contingent valuation methods. *Journal of the Korea Institute of Information Security and Cryptology, 22*(2), 367-377.

[16] Lipovetsky, S., and Conklin, W. (2015). AHP priorities and the markov-chapman-kolmogorov steady-states probabilities. *International Journal of the Analytic Hierarchy Process, 7*(2), 349-363.

[17] Liu, C., Ang, R. P., and Lwin, M. O. (2016). Influences of narcissism and parental mediation on adolescents' textual and visual personal information disclosure in Facebook. *Computers in Human Behavior, 58*, 82-88.

[18] McCallister, E., Grance, T., and Scarfone, K.A. (2010). SP 800-122-Guide to protecting the confidentiality of personally identifiable information, Technical Report.

[19] Montes, R., Sand-Zantman, W., and Valletti, T. (2015). The value of personal information in markets with endogenous privacy (No. 851). Institut d'Économie Industrielle (IDEI), Toulouse.

[20] Nowak, G. J., and Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing, 9*(3), 46-60.

[21] Park, K. A., Lee, D. Y., and Koo, C. (2014). A Study on the Effect of Location-based Service Users' Perceived Value and Risk on their Intention for Security Enhancement and Continuous Use: With an Emphasis on Perceived Benefits and Risks. *Asia Pacific Journal of Information Systems, 24*(3), 299-323.

[22] Park, J., Kewon, E., Park., M, and Chai, S. (2017). The Value of Private Information based on Cost-Benefit Analysis Framework: Focusing on Individual Attributes, Dealer Traits, and Circumstantial Properties. *Information Systems Review, 19*(3), 155-177.

[23] Phelps, J., Nowak, G., and Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

[24] Saaty, T. L. (1977). A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology, 15*(3), 234-281.

[25] Saaty, T. L. (1994). How to make a decision: The analytic hierarchy process. *Interfaces, 24*(6), 19-43.

[26] Saaty, T. L. (2003). Decision-making with the AHP: Why is the principal eigenvector necessary. *European Journal of Operational Research, 145*(1), 85-91.

[27] Schoch, T. P. (2016). EU privacy regulations' impact on information governance. *Information Management Journal, 50*(1), 20-25.

[28] Shinyoung Park, "Financial related personal information Commercial transactions must be allowed", 2018.03.30, Retrieved from http://news.hankyung.com/article/201803308

[29] Simoens, K., Bringer, J., Chabanne, H., and Seys, S. (2012). A framework for analyzing template security and privacy in biometric authentication systems. *IEEE Transactions on Information Forensics and Security, 7*(2), 833-841.

[30] TAHAOĞLU, O. O. (2009). Personal data protection in Turkey: An information technology framework indented for privacy risk management (Doctoral dissertation, DEÜ Fen Bilimleri Enstitüsü).

[31] Tasidou, A., Efraimidis, P. S., and Katos, V. (2009). Economics of personal data management: Fair personal information trades. *International Conference on E-Democracy*, 151-160.

[32] Terzi, D. S., Terzi, R., and Sagiroglu, S. (2015). A survey on security and privacy issues in big data. In *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference* (pp. 202-207). IEEE.

[33] Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly, 33*(3), 472-480.

[34] Wind, Y., and Saaty, T. L. (1980). Marketing applications of the analytic hierarchy process.

Management Science, 26(7), 641-658.

[35] Yoo, J., Jie, S. H., and Lim, J. (2009). Estimating Direct Costs of Enterprises by Personal Information Security Breaches. *Journal of the Korea Institute of Information Security and Cryptology, 19*(4), 63-75.

[36] Yu, M. M., Ting, S. C., and Chen, M. C. (2010). Evaluating the cross-efficiency of information sharing in supply chains. *Expert Systems with Applications, 37*(4), 2891-2897.

[37] Personal Information Definition. Retrieved February 21, 2018, from www.PrivacySense.net

[38] Chosunbiz, 2018.02.17 Retrieved from http://biz.chosun.com/site/data/html_dir/2017/02/17/2017021701092.html?rsMobile=false

[39] Yonhapnews, 2016.07.28 Retrieved from http://www.yonhapnews.co.kr/bulletin/2016/07/27/0200000000AKR20160727136900002.HTML

◆ About the Authors ◆

Minjung Park

Minjung Park is Ph.D candidate of Ewha School of Business, Ewha Womans University. She received B.S from the college of Law in Sungshin Women's University and M.S in Data Analytics from Ewha Womans Univeristy. Her research interest is behavioral information security, information security management, privacy and Blockchain.

Sangmi Chai

Sangmi Chai is an Associate Professor in Ewha School of Business, Ewha Womans University. She received her PhD in MIS from School of Management, State University of New York at Buffalo. She was an Assistant Professor in College of Business, Information and Social Sciences, Slippery Rock University, PA, USA. She graduated from MBA in Seoul National University and received BS in the Ewha Womans University. Her research interests include information privacy and security, trust and knowledge management, and IT investment.

Submitted: April 10, 2018; 1st Revision: June 12, 2018; Accepted: August 1, 2018