Strategic Approach to Privacy Calculus of Wearable Device User Regarding Information Disclosure and Continuance Intention

Ji Yeon Cho[1], Daesun Ko[2] and Bong Gyou Lee[1]
[1] Graduate School of Information, Yonsei University
Seoul, South Korea
[e-mail: jy.cho, bglee@yonsei.ac.kr]
[2] Department of Sports and Lesiure Studies, Yonsei University
Seoul, South Korea
[e-mail: golds9393@hanmail.net]
*Corresponding author: Bong Gyou Lee

Received October 16, 2017; revised February 19, 2018; accepted March 6, 2018; published July 31, 2018

Abstract

The healthcare and fitness wearable-device market is considered as the driving force of the entire wearable device market. However, there are concerns with respect to information privacy because wearable devices constantly collect sensitive data such as individuals' health information. Thus, there is a need for a comprehensive understanding from the perspective of information privacy concerns and related behavior. This study investigates factors considered in the privacy calculus of wearable fitness devices, and verifies differences obtained by the privacy calculus process according to the frequency of exercise. The results obtained from a survey of 248 undergraduate students in Korea revealed that service providers should consider users' interests and exercise characteristics in order to mitigate their privacy concerns and encourage continuous use of wearable devices. This study provides useful insights pertaining to users of wearable fitness devices, and targets researchers and practitioners.

Keywords: Wearable device & service, Information privacy concern, Privacy calculus, Information disclosure, Continuance intention

1. Introduction

With the development of wearable technology, the use of wearable devices has gradually spread to everyday life. Beginning with smart bands, wearable technologies have been applied in various forms and fields such as clothing, health services, and the medical field. According to the market research firm IDC, in 2016, the wearable device market was expected to grow at a compounded annual growth rate of 20.3% over the next five years. Currently, competition in the wearable device market is focused primarily on the fields of healthcare and fitness [1]. Samsung Electronics, which leads the wearable device market in Korea, is also focusing on the health care market [2] because consumers are more interested in managing their own health by quantifying their health data, with the aim of achieving prevention-oriented wellness. However, as the number of wearable-device users increases, the security of constantly generated personal information as well as privacy concerns have raised serious social issues. Since the development of the mobile business environment, the process of encouraging users to consent to share their information has become a strategic area that should be addressed before businesses can provide personalized services to customers [3]. However, users whose wearable devices generate personal information have begun to recognize the potential for personal information leakage. According to a Price Waterhouse Coopers report, survey respondents replied that privacy is one of the reasons they hesitate to purchase fitness bands [4]. Most wearable devices require regular synchronizing with smart phone apps that enable tracking a user's location and monitoring activity data. Based on the service structure of wearable devices, user data collected by devices are analyzed and subsequently transmitted via an application that is linked to a smartphone. In this manner, continuous management-related and personalized services are provided to users, and there has been accelerated research into the privacy issues over the past few years. Edith Ramirez, America's top privacy regulator, said she will not use Fitbit, one type of wearable device, because she does not want her sensitive information to be monitored [5]. Recently, these privacy related concerns have expanded from personal concerns to social issues. Fitness tracking information including location data has revealed government secrets such as the location of sensitive government facilities [6]. Accordingly, information privacy is becoming a concern to multiple stakeholders, including business operators, privacy activists, researchers, government regulators, and individual consumers. If wearable devices cause serious privacy invasion, many users will abandon their wearable devices or stop providing their personal data. However, the services provided for a wearable device are not possible without data synchronization, so protecting privacy is an important issue to be solved. Based on initial studies on wearable devices, researchers have focused on identifying factors that affect users' intentions to use a device or acceptance of the technology [7], and initial studies regarding privacy in wearable devices tend to explore factors that affect the privacy concerns of potential users and which are related to technical issues. However, the wearable fitness device market has matured, and research focusing on privacy factors that affect actual users' intentions to disclose information and to continue the use of wearable devices is needed. In addition, although the main functions of wearable fitness devices are related to exercise data management, existing studies have not been sufficiently validated to determine the influence of exercise or health-related variables on user acceptance.

To address the above limitations, this study aims to verify the antecedents of privacy calculus theory and to identify the causal relationship between the intention to disclose

information and a continuance intention to use the device from an expanded view. Previous studies confirmed the rationale for the perceived usefulness and performance expectancy of wearable devices to differ according to health awareness [8, 9]. Based on the theoretical aspect of the prior study, our study also examined whether there is a difference in the privacy calculus process depending on the frequency of exercise. The contribution of this study lies in its focus on examining the privacy calculus for different individuals, as reflected by the frequency of their personal exercise regime. The remainder of this study is organized as follows. Section 2 reviews the information privacy issues related to wearable devices as well as literature on privacy calculus theory. Section 3 addresses the hypotheses of this study, while section 4 presents the methodology. Section 5 presents the analysis results and their implications, and we discuss the limitations of this study in Section 6.

2. Literature Review

2.1 Wearable Devices and Information Privacy Concern

With the significant developments in wearable technology, there has been increased usage of various forms of advanced wearable devices and associated services. There are largely four types of wearable devices according to their intended use and function, namely fitness and wellness, healthcare and medical, infotainment, and industrial and military [10].

Wearable devices are instruments that can be worn on the body of a user, and they monitor the user at the contact position with the user's body. These wearable devices have allowed the collection of extremely detailed information pertaining to an individual user's life, including health, location, movement, and daily activities. In this process, privacy invasion and data leakage while generating and collecting data using wearable technology have been identified as issues that should be urgently addressed in the wearable device industry. In particular, fitness/healthcare wearable devices collect personal information including vital signs and activity data, which are very personal and sensitive to consumers. However, studies conducted during the early developmental stages of wearable devices have focused on technical issues such as determining factors that affect the intention to use devices or related services [1, 10, 11]. Currently, as the issue of the misuse of privacy data is emerging, it is necessary to study the relationships among privacy concerns of consumers, personal information disclosure, and the use of wearable devices and services.

Studies on privacy concerns have investigated the factors related to the direct or indirect causal relationships between privacy concerns and information disclosure/intention to use (behavioral intention) [12]. With the changes in IT services, these studies have been verified to various degrees, and then expanded to test such factors in the internet and mobile environments [13, 14, 15, 16, 17, 18]. Smith et al. [13] developed a Concern for Information Privacy (CFIP) model, which identifies four dimensions of privacy concerns: collection, secondary use, errors, and improper access to personal information According to Smith et al. [13] privacy concerns are regarded as "individuals' concerns about organizational information privacy practices" (p. 169). Stewart et al. revalidated the CFIP model empirically [14]. The scale of CFIP has been widely applied in different contexts and various fields such as SNS marketing, online commerce, and healthcare [19]. Then, in a later study on users in an online environment, Malhorta et al. expanded such concepts, and proposed the Internet Users Information Privacy Concern (IUIPC), which could measure the level of information privacy concerns of Internet users based on the CFIP model [15]. IUIPC is a model that has strengthened the concept of the "right to informational self-determination" based on studies by

Smith et al. and Stewart et al. [13, 14]. Then, based on an idea that mobile users were different from online users, Xu et al proposed the Mobile Users' Information Privacy Concern (MUIPC) model, where the information privacy concerns of mobile users were composed of three dimensions, i.e., perceived surveillance, perceived intrusion, and secondary use of information, and conducted empirical studies [18].

Based on the discussions to date, studies related to information privacy concerns have been applied in different ways according to the status of service use by users and the nature of the IT services. Thus, it is necessary to investigate the factors and the causal relationships of information disclosure that result in information privacy concerns for users of wearable devices, for which the nature of collected data and the user environment significantly differ.

2.2 Privacy Calculus Theory

This study extends privacy calculus theory to examine one's intention to disclose information and the continued use of wearable devices by users. The privacy calculus model, which was developed by Laufer and Wolfe, is used to explain consumer behaviors and privacy perception [20]. Laufer and Wolfe first used this terminology as an aspect of personal information management, as a calculus of the behavior, and the privacy calculus model was later applied in the information systems (IS) field by Culnan and Armstrong [21]. Although there exist various concepts of information privacy, there is little difference in operationalizing information privacy in the information systems (IS) field [18]. Information privacy concerns have become an important aspect of IS research, and to date, many privacy-related studies such as e-commerce, location-based services (LBS), mobile devices, and wearable devices have been developed using the privacy calculus model [16, 22, 23].

Information privacy is classified as four definitional approaches: privacy as a human right, privacy as a commodity, privacy as a state of limited access, and privacy as the ability to control information about one's self [19, 24]. The theory of privacy calculus has evolved not from the perspective of one's absolute right of inviolability, but as a commodity that determines circumstances with maximum benefit and minimal loss. Prior studies that applied the privacy calculus model evaluated results of the intention to disclose customers' personal information by comparing the perceived risk and expected benefit. Factors of benefit and risk were verified separately, either as a single dimension, or as multidimensional concepts, and various theories were also applied according to the purpose of the study [25, 26]. According to Keith et al. [16], "If information privacy is a commodity, then an individual's decision to disclose versus retain information privacy can be framed as a rational choice (Becker and Murphy, 1988) made by weighing the costs and benefits of disclosure" (p. 1164). Therefore, various theories, such as the theory of reasoned action (TRA) [27] and the theory of planned behavior (TPB) [28] are also applied to determine the relationships between information privacy concerns and factors related to IT users' attitudes, beliefs, intentions, and behaviors. Further, in the study by Li, various theories were reviewed from different perspectives to determine how the privacy calculus is operated. When scholars use the privacy calculus theory, they incorporate other theories such as the utility maximization theory, the expectancy theory of motivation, and the expectancy-value theory to develop the trade-off functions [26]. Therefore, this study verifies factors that affect the intention to disclose personal information of wearable device users, and the relationship between the intention to disclose information and the ongoing intention, by applying the privacy calculus model from a cost-benefit perspective.

3. Research Model and Hypotheses

Users decide to disclose information using a privacy calculus that involves tradeoffs among several contrasting factors such as trust, benefit, and privacy risk [21, 22]. Privacy calculus is a complete mental calculation process involving multiple considerations, and to examine important factors, additional theories are applied [26]. Thus, this study adopted privacy calculus theory as the overarching theory from which a research model is developed.

3.1 Privacy Calculus

Privacy calculus theory postulates that individuals perform a calculus between the expected loss of privacy and the potential gain of disclosure, and their final decision is determined by the outcome of the privacy trade-off [22, 24, 29]. To explain the trade-off in the mental calculation in the wearable device context, the research model employed in this study includes the perceived value of information disclosure and perceived information privacy concern. To present a balanced view, Wang et al. (2016) also tested the research model, including antecedents of both the perceived benefit and the privacy risk. Thus, we hypothesize that the decisions by users of wearable devices regarding disclosure intentions are determined by tradeoffs between their perceived privacy concern and the perceived value [3].

Perceived value is an important concept that is applied in the field of marketing and information systems. It has been used as a critical single or multidimensional factor that significantly impacts the intention to use and obtain satisfaction [24, 30, 31, 32]. In the privacy calculus of information disclosure, Xu et al. [24]. defined the perceived value of information disclosure as “the individual's overall assessment of the utility of information disclosure based on perceptions of privacy risks incurred and benefits received” (p. 44). In the notion of the privacy calculus theory, the concept of perceived value is similar to the process of risk-benefit analysis, which considers various factors pertaining to information disclosure. That is, most scholars have excluded value as an explicit latent construct in the privacy calculus model. However, Morosan & DeFranco argued that the notion of value was incorporated in the conceptualization of benefits, and perceived value is critical to complete the privacy calculus model and to verify the perceived value of disclosure as the predictor(s) of willingness to disclose personal information [33]. In this study, perceived value is considered as a predictor of one’s intention to disclose information. Based on existing studies, we have defined the perceived value as the user’s overall assessment of the utility of a wearable device based on perceptions of information disclosure [16, 24, 31]. Accordingly, the following hypothesis was developed.

Hypothesis 1. Perceived value is positively related to the intention to disclose information.

Privacy calculus assumes that users' behavioral intentions and actions are affected by both positive and negative factors such as the expected utilities and the estimated costs of a potential privacy violation.[21]. Privacy concerns are among the most widely used variables in IS research, and are consistently shown to be one of the strongest predictors of privacy-related behavior [29]. We include the factor of perceived privacy concern as a privacy risk position in the privacy calculus model, which involves a user’s awareness of privacy invasion or risk related to information disclosure. In information privacy research, privacy concerns are opposite to perceived benefit factors in the privacy calculus process, and they are similar to the relationship of perceived cost/risk [26]. In other words, the relationship between perceived

concern and the intention to disclose information has been verified [16, 34]. It was demonstrated that privacy concerns affect not only information disclosure, but also have a causal effect on value (benefit). Xu et al. reported that in management literature, the risk is positively related to the value, and if consumer aware the existence of high risks of privacy invasion, assessments of the utility of information disclosure will be low [24]. Xu et al. also hypothesized that the perceived privacy risk of information disclosure is negatively related to the perceived value. Li et al. verified the hypothesis that the perceived benefit reduces the perceived privacy risk [1]. Hence, we set the hypotheses to consider the relationships between perceived privacy concern, intention to disclose information, and perceived value as follows.

Hypothesis 2. Perceived privacy concern is negatively related to the intention to disclose information.

Hypothesis 3. Perceived privacy concern is negatively related to the perceived value.

In most of the previous studies on IT services, privacy-related factors affecting users' willingness to disclose personal information and variables affecting users' intentions to accept a device have been separately verified. However, because information is collected and privacy data are provided continuously when using recently developed smart device-based services, it is necessary to conduct a study on the intention to disclose information and the use behavior from an integrated perspective. In this context, Weinhard & Hauser proposed a model that applied a combination of the Unified Theory of Acceptance and Use of Technology (UTAUT2) and the privacy calculus theory, and they studied the intention to accept the retail system and the willingness to provide information [34]. Their study found that there was a causal relationship between the willingness to provide personal information and the behavioral intention to use the system. In the wearable device use context, it is very important to verify the existence of the relationship between the intention to disclose information and the intention toward continued use, because sensitive data are collected continuously during use, even after the wearable device has been accepted to user. Wearable devices collect more sensitive information (such as body data) than conventional smart devices to provide personalized services through the application. Therefore, in this study, the causal relationship between the intention to disclose personal information and continuance intention was investigated. Park also confirmed the impact of a person’s willingness to provide location data on the intention for sustainable use [23]. Therefore, this study defined the intention to disclose information as a user’s intention to disclose personal information during the use of a wearable device, and the continuance intention as the user’s intention to continue using a wearable device [32], and set up the following hypothesis.

Hypothesis 4. Intention to disclose information is positively related to continuance intention.

3.2 Antecedents of Privacy Calculus

Our research aims to verify the factors of privacy calculus in the wearable device context. First, we consider the perceived enjoyment and perceived usefulness as factors of perceived value. Kim et al. proposed usefulness and enjoyment as the most representative factors of the perceived value in the mobile internet context, and argued usefulness as an extrinsic and cognitive benefit, and enjoyment as an intrinsic and affective benefit [31].

In previous studies, the concept of enjoyment is similar to that of emotional value. Perceived enjoyment involves defining emotional feelings such as joy or pleasure that a product generates [31]. Based on previous studies, this study defines the perceived enjoyment

as the factors of perceived value that means using wearable devices are perceived as being enjoyable [31, 35]. Davis et al. explained that for users who experience pleasure or joy from using a technology enjoyable in its own right (aside from the instrumental value), they tend to adopt the technology and use it more extensively than others [31, 36]. Past studies have also confirmed that the benefit component comprises perceived enjoyment, and enjoyment follows usefulness as an important variable in the technology-acceptance context [31, 35].

Davis [37] suggested perceived usefulness as an important variable in the technology acceptance model (TAM) that affects the acceptance and satisfaction of technology and service in IT issues. Perceived usefulness, which is defined as the ‘‘degree to which a person believes that using a particular system would enhance his or her job performance” (p. 320) [37], has been regarded as influential factors of IT adoption [35]. In this study, usefulness is defined as the degree to which a person believes that using wearable devices will enhance exercise performance. Wearable devices users believe that they can improve their exercise performance by checking their information regarding their schedule and by communicating with other users anytime, anywhere. Therefore, we hypothesize that the usefulness and enjoyment of wearable devices will positively affect the overall perceived value as one of its advantages, and we introduce the following hypotheses.

Hypothesis 5. Perceived enjoyment is positively related to perceived value.

Hypothesis 6. Perceived usefulness is positively related to perceived value.

Second, we verify the factors related to perceived privacy concerns. The IUIPC model proposed by Malhotra et al. [15] classify privacy concerns into three dimensions, namely collection, control over personal information, and awareness of organizational privacy practices, and it has empirically shown that the predictor of CFIP has an impact on the threats to the privacy of online users. Based on previous studies, concerns related to information privacy in mobile users [17, 18] were studied, and were largely classified into three factors, namely the secondary use of personal information, perceived surveillance, and perceived intrusion. MUIPC reflects characteristics of mobile services such as aggressive data collection activities performed by mobile apps [18].

This study presented a hypothesis that identifies factors of perceived surveillance and the secondary use of personal information as the risk components of perceived privacy concerns in the wearable device use context. In a study by Bae et al., users' privacy concerns were examined in the Internet of Things (IoT) context, and only the hypotheses of the “risk on technology” and “risk on service providers” had an impact on the perceived privacy risk. These two factors are similar to the constructs employed in our study, except for the trust based on legislation [38]. The result obtained by Bae et al. is similar to that of Chae et al. [30]. Only two hypotheses (“risk of technology” and “risk of service providers”), with the exception of the risk of regulation were supported [30]. This result may be attributed to the technical characteristics of smartphones. In today’s “smart” environment, vendors have effective surveillance technologies that can track and profile users. Users of wearable devices may be concerned that their activities while using wearable devices may be constantly recorded and transmitted to various vendors. Heng Xu et al. noted that the rapid development of mobile technologies has expanded the means of surveillance because of active data-collection activities that are now possible using technology, and mobile vendors are constantly monitoring user behavior through mobile devices [18]. Wearable devices have various functions, such as location monitoring, tracking movements, and can collect more personal sensitive data than other personal devices. According to Solove [39], surveillance is “the watching, listening to, or recording of an individual’s activities” (p.490). Accordingly, we

include perceived surveillance as an important factor that affects the perceived privacy concern.

The secondary use of personal information can be defined by the concern that information is collected for one purpose but is used for another, secondary purpose, after disclosure to a third party (not the collecting entity) without authorization from the users [13]. According to previous privacy-related studies, the secondary use of personal information without agreement to disclosure, invades consumers' privacy of information [40]. In addition, consumers with a high level of privacy invasion concern do not agree with companies using their personal information, leading to vigorous consumer objections. The using consumer data without individual's permission was considered as a privacy invasion and the secondary use of personal information causes strong consumer objections potentially [41]. Solove [39] explained that, "The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability" (p. 522). Accordingly, users' perceived privacy concerns increase when there is a secondary use of personal information without users' consent. Chae et al. verified that privacy concerns involving IoT service providers has affected persons' intention to use smart wearable devices [30]. Hence, we hypothesize:

Hypothesis 7. Perceived surveillance is positively related to perceived privacy concern.

Hypothesis 8. Secondary use of information is positively related to perceived privacy concern.

Previous studies on wearable fitness devices have not adequately covered the causal relationships of variables, such as interest in exercise or the amount of exercise. Thus, this study aims to find the difference in the privacy calculus process between groups according to the frequency of exercise. Existing studies pertaining to the acceptance of health-related wearable technology included health consciousness and personal traits as antecedents [1, 8, 11]. Health consciousness refers to a given level of interest in personal health, and is reflected by voluntary searches for health-related information as well as efforts to consistently put them into practice [8, 11]. If health consciousness is high, interest in health information is also high, and we can predict the possibility of pursuing health information actively [42]. Shin and Lee revealed that health consciousness had a significant impact on the intention to purchase wearable devices, and Kim and Kim confirmed that a group using smartphone applications realized greater improvements in terms of the amount of exercise and training than groups that did not use smartphone applications [8, 43].

In addition, Kong suggested that a group using the healthcare home-smart exercise program showed improvement in the reduction of waist circumference and abdominal obesity compared with a group that performed general exercise [44]. In other words, it can be conceived that wearable device users in a high-exercise group are more likely to exhibit health-oriented behaviors by using wearable devices. Based on prior studies, this study investigated the hypothesis that there is a difference in the intention to disclose information and the continuance intention to utilize wearable devices in order to enhance the enjoyment and efficiency of exercise, depending on the frequency of exercise.

Hypothesis 9. Factors of privacy calculus will vary depending on the frequency of exercise.

4. Methodology

4.1 Sample and Survey Design

Because the main consumer group of wearable devices is the young generation, the study selected university students as survey participants. The survey was administered to undergraduate students at three large universities located in South Korea. The total number of questionnaires collected was 259, excluding those with invalid responses. The statistical results of 248 valid responses were then assessed from the survey, and are shown in **Table 1**.

All selected respondents are actual users of wearable devices, and participate in physical education classes. The type of wearable device worn by respondents is a wrist-mounted device called a fitness band or smart watch. Fitness bands collect users' activity data including sleep pattern, calories burned, heart rate, and running location route. This type of device is less sensitive regarding private information than head-mounted devices such as Google Glass but are more commercialized [45]. However, if a user wants more personalized and advanced functions with a wrist device, more details are required such as birthday, gender, height, weight, and contact information. In this study, the characteristics of the fitness band and the required information are mentioned in the questionnaire.

This research utilizes covariance-based structural equation modeling to validate the hypotheses, and SPSS 15.0 and Amos 18.0 were used as analysis tools. The process of analysis is as follows. First, exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) were performed to verify the fitness measurement model, and ultimately to verify the reliability and convergent validity of the measurement tools [46]. Next, the correlation of latent variables was analyzed and the discriminant validity was verified by a constraint test. Once the fit indices of the structural model were confirmed, the validation of the hypothesis took place. All survey items were adapted from the existing studies to fit our research context, and were assessed using a 5-point Likert scale ranging from 1 ("strongly disagree") to 5 ("strongly agree"). **Table 2** presents the summary of measurement items.

4.2 Reliability and Validity of Measurement Tools

An EFA was employed using principal component analysis with varimax rotation. Factor extraction was based on the existence of eigenvalues higher than 1, with the requirement that the factorial loadings were higher than 0.4, and a significant total explained the variance [47].

Table 1. Characteristics of the sample participants

Demographics	Category	Frequency	Percentage (%)
Gender	Male	162	65.3
	Female	86	34.7
Age	Under 20	52	21
	21-23	111	44.8
	Above 24	85	34.3
Preferred Type of Exercise	Individual sports	127	51.2
	Team sports	121	48.8
Average of Monthly Exercise	9 times or less	125	50.4
	10 times or more	123	49.6

Table 2. Measurement items

Constructs	Items	Descriptions
Perceived Value [24, 31, 33]	PV1	Compared to the risks of my information disclosure., the use of a wearable device is beneficial to me
	PV2	Compared to the information I need to disclose, the use of a wearable device offers value to me
	PV3	Overall, the use of a wearable device delivers good value to me
Privacy Concern [22, 48]	PPC1	I am concerned that my information collected by the wearable device could be misused.
	PPC2	I am concerned about providing my information to use a wearable device, because it could be used in a manner I did not foresee
	PPC3	I am concerned about submitting information to a wearable device, because of what others might do with it
Intention to Disclose Information [24, 33]	IDI1	I am likely to disclose my information by using a wearable device
	IDI2	I am interested in disclosing my information to the wearable device
	IDI3	I intend to continue to provide my information
	IDI4	I am willing to disclose my information to continue use of my wearable device
Continuance Intention [23, 32, 37]	CI1	I predict that I will continue using a wearable device in the near future
	CI2	If I could, I would like to continue using wearable devices
	CI3	I intend to continue using wearable devices
	CI4	I intend to regularly use a wearable device
Perceived Enjoyment [31, 35]	PE1	Using wearable devices is fun
	PE2	A wearable device gives me more pleasure in exercise
	PE3	I enjoy using my wearable device
Perceived Usefulness [35, 37]	PU1	Wearable devices are very useful to my exercise
	PU2	Wearable devices provide very useful service and information to me
	PU3	Using wearable device improves the quality of the exercise
Perceived Surveillance [18]	PS1	I am concerned that wearable devices are collecting too much information (activity, physical data) about me
	PS2	I am concerned that wearable devices may monitor my activities
	PS3	I believe that information in my wearable device is monitored at least part of the time
Secondary Use of Information [13, 18]	SUI1	I am concerned that wearable devices may use my information for other purposes without notifying me or asking for my authorization
	SUI2	When I give my information to a wearable device, I am concerned that the wearable device may use my information for other purposes
	SUI3	I am concerned that wearable devices may share my information with others without obtaining my authorization

Through the EFA, two measurements, PS3 and PPC3, which resulted in low factor loading values, were excluded. For the EFA results: the perceived value factor loadings ranged from 0.714 to 0.866, the perceived privacy concern factor loadings ranged from 0.843 to 0.879, the intention to disclose information factor loadings ranged from 0.768 to 0.896, the continuance intention factor loadings ranged from 0.724 to 0.895, the perceived enjoyment factor loadings ranged from 0.757 to 0.848, the perceived usefulness factor loadings ranged from 0.685 to 0.812, the perceived surveillance factor loadings ranged from 0.843 to 0.871, and the secondary use of information factor loadings ranged from 0.879 to 0.885. To verify the goodness of fit of the inventory, the CFA, reliability, and construct validity were analyzed and the results are shown in **Table 3**.

Table 3. Results of convergent validity and reliability testing

Variable	Item	S. Loading	S.E	C.R	AVE	Cronbach-α
Perceived Value	PV1 PV2 PV3	0.803 0.788*** 0.799***	 0.082 0.075	- 13.084 13.026	0.738	0.839
Perceived Privacy Concern	PPC1 PPC2	0.898 0.795***	 0.087	- 13.833	0.812	0.832
Intention to Disclose Information	IDI1 IDI2 IDI3 IDI4	0.859 0.884*** 0.901*** 0.811***	 0.050 0.054 0.060	- 20.367 18.538 16.639	0.768	0.920
Continuance Intention	CI1 CI2 CI3 CI4	0.876 0.917*** 0.873*** 0.783***	 0.051 0.054 0.060	- 20.808 18.919 15.506	0.745	0.919
Perceived Enjoyment	PE1 PE2 PE3	0.816 0.839*** 0.816***	 0.068 0.072	- 14.399 13.960	0.818	0.863
Perceived Usefulness	PU1 PU2 PU3	0.700 0.720*** 0.703***	 0.099 0.091	- 9.128 9.096	0.798	0.749
Perceived Surveillance	PS1 PS2	0.866 0.742***	 0.117	- 9.877	0.832	0.782
Secondary Use of Information	SUI1 SUI2 SUI3	0.902 0.871*** 0.885***	 0.050 0.049	- 19.204 19.732	0.843	0.916

***p<.001

By examining the fit indices of the measurement model, we obtained $\chi 2$ = 430.990, df = 224, RMSEA = 0.06 (<0.08), RMR = 0.03 (<0.05), CFI = 0.95 (>0.90), TLI = 0.938 (>0.90), and NFI = 0.902 (>0.90), which are sufficient to fulfill a measurement model's overall construct validity. Then, the convergent validity and reliability analysis indicated that the standardized factor loading values were mostly above the standards [46]. The standard error (S.E), critical ratio (C.R), average variance extracted (AVE) values, and Cornbach's Alpha of variables were all above the standard value, meaning that the survey elements had appropriate convergent validity and reliability.

4.3 Correlation

A correlation analysis was conducted to examine the relationships among the perceived value, perceived privacy concern, intention to disclose information, continuance intention, perceived enjoyment, perceived usefulness, perceived surveillance, and secondary use of information. The results showed that statistically significant correlations existed among variables of positive or negative correlations. Also the square root of AVE should be greater than the correlation between a pair of constructs [49].

Table 4. Correlation analysis

	Mean(S.D)	PV	PPC	IDI	CI	PE	PU	PS	SUI
PV	3.44(0.72)	**0.86**							
PPC	3.54(0.91)	-0.09	**0.91**						
IDI	2.80(0.90)	0.32**	-.30**	**0.88**					
CI	3.03(0.86)	0.42**	-0.13*	0.59**	**0.86**				
PE	3.51(0.84)	0.37**	0.03	0.33**	0.37**	**0.90**			
PU	3.61(0.72)	0.55**	-0.07	0.24**	0.41**	0.48**	**0.89**		
PS	3.50(0.94)	0.02	0.55**	-0.19**	-0.05	0.13**	0.05	**0.91**	
SUI	3.34(0.94)	0.04	0.62**	-0.39**	-0.12	-0.01	-0.01	0.48**	**0.92**

Note: PV: Perceived value, PPC: Perceived privacy concern, IDI: Intention to disclose information, CI: Continuance Intention, PE: Perceived enjoyment, PU: Perceived usefulness, PS: Perceived surveillance, SUI: Secondary use of information (bold number show square roots of AVE for that construct, **p<.01)

Because the square root of AVEs in the diagonal (values in bold face) are greater than the values in their corresponding row and column (see **Table 4**), we can conclude that discriminant validity is obtained for the measures in this study.

5. Analysis of Result

With respect to the result to confirm the suitability of the total structural model, $\chi 2/df = 2.391$ ($\chi 2 = 569.026$, df = 238) was lower than 3. The fit indices of other structural models were RMSEA = 0.075, RMR = 0.084, CFI = 0.920, TLI = 0.907, and NFI = 0.870. Among these, TLI, CFI, and RMSEA, previously used in the reference studies, were also used in order to analyze the theoretical structure model and test its goodness of fit. The indices for measuring goodness of fit were used because they were not significantly influenced by the sample size, yet they were adequate for considering the model's parsimony [50]. Therefore, it was found that the goodness of fit of the model was acceptable in this study. **Fig. 1** shows analysis results of the hypotheses obtained using structural equation modeling (SEM) [51].

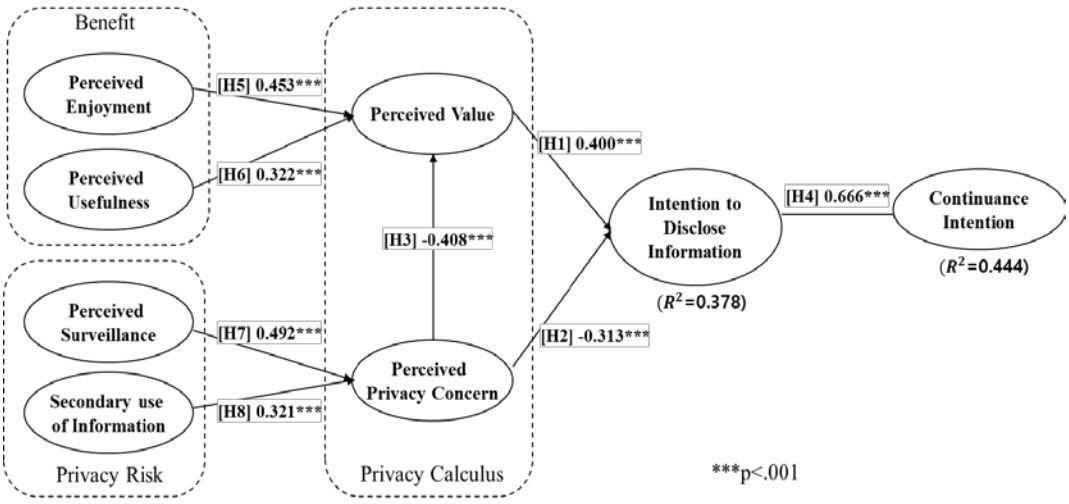

Fig. 1. Results of total structural equation modeling

To summarize the validation results, eight hypotheses (H1, H2, H3, H4, H5, H6, H7, and H8) were supported. Detailed validation results are as follows. First, H1 is validated (path coefficient = 0.400, t = 5.404) as the perceived value was found to positively impact (+) the intention to disclose information. Second, H2 is validated (path coefficient = -0.313, t = -4.339) as the perceived privacy concern was found to negatively impact (-) the intention to disclose information. In addition, the perceived privacy concern was found to negatively impact (-) the perceived value, validating H3 (path coefficient = -0.408, t = -6.951). Third, H4 is validated (path coefficient = 0.666, t = 10.671) as the intention to disclose information was found to positively impact (+) the continuance intention to use. Fourth, both the perceived enjoyment (path coefficient = 0.453, t = 5.387) and perceived usefulness (path coefficient = 0.322, t = 3.660) positively impacted (+) the perceived value, validating H5 and H6. Finally, both the perceived surveillance (path coefficient = 0.492, t = 5.657) and secondary use of information (path coefficient = 0.321, t = 4.310) positively impacted (+) the perceived privacy concern, validating H7 and H8.

To examine the different factors of privacy calculus according to exercise properties, we divided user groups into low-exercise and high-exercise groups based on the mean exercise frequency of the sample. The mean exercise frequency of our study was 10 times per month thus samples were divided into a group exercising nine or fewer times per month (low-exercise group) and a group exercising 10 or more times per month (high-exercise group).

The SEM difference between groups according to the frequency of exercise is as follows. First, with respect to the result of confirming the appropriateness of the structural model for the low-exercise group, $\chi 2/df$ = 1.829 ($\chi 2$ = 435.229, df = 238) was lower than 3. The fit indices of other structural models were RMSEA = 0.082, RMR = 0.097, CFI = 0.909, TLI = 0.895, and NFI = 0.822, where some figures do not satisfy the threshold values. However, for RMSEA, TLI, and CFI the goodness of fit of the study model was acceptable. The result to confirm the suitability of the structural model in the high-exercise group resulted in $\chi 2/df$ = 1.646 ($\chi 2$ = 391.707, df = 238), which was lower than 3 and relatively ideal value. The fit indices of other structural models were RMSEA = 0.073, RMR = 0.060, CFI = 0.925, TLI = 0.913, and NFI = 0.832, where the figures satisfy the threshold values. In summary, the CFA result validated the model fit for both groups according to the frequency of exercise. **Table 5** shows the path coefficient of the SEM of both the low-exercise and high-exercise groups.

Table 5. Results of SEM in low-exercise group and high-exercise group

Path	Low-exercise group (N=125)		High- exercise group (N=123)	
	Path coefficient	S.E	Path coefficient	S.E
PV→ IDI	0.335**	0.157	0.451***	0.177
PPC → IDI	-0.293**	0.094	-0.318*	0.140
PPC → PV	-0.364***	0.050	-0.471***	0.070
IDI → CI	0.611***	0.078	0.769***	0.092
PE → PV	0.497***	0.080	0.324**	0.017
PU → PV	0.245*	0.130	0.332**	0.128
PS → PPC	-0.018	0.119	1.029***	0.140
SUI → PPC	0.730***	0.111	-0.069	0.072

Note: PV: Perceived value, PPC: Perceived privacy concern, IDI: Intention to disclose information, CI: Continuance intention, PE: Perceived enjoyment, PU: Perceived usefulness, PS: Perceived surveillance, SUI: Secondary use of information, *p<.05, **p<.01, ***p<.001

Table 6. Results of comparison testing between subgroups based on exercise frequency

Hypothesis	Path	Low-exercise group (N=125)		High-exercise group (N=123)		t-value
		Path coefficient	S.E	Path coefficient	S.E	
H9	PS → PPC	-0.018	0.119	1.029***	0.140	-5.698***
	SUI → PPC	0.730***	0.111	-0.069	0.072	6.039***

Note: PS: Perceived surveillance, PPC: Perceived privacy concern, SUI: Secondary use of information ***p<.001

We further tested whether the difference of path coefficients for the two groups is significantly different by calculating the pooled estimator for the variance, sample size of the two groups, and t-distribution with degrees of freedom [52]. To test whether the difference of path coefficients for two groups is significant, we calculate the t-value. We applied the Smith-Satterthwaite test (see Formula (1)) that does not assume normal distribution for this test [53].

$$t = \frac{P_{sample1} - P_{sample2}}{\sqrt{S.E^{2(sample1)} + S.E^{2(sample2)}}}, \quad \mathrm{df} = M + N - 2 \qquad (1)$$

Note: P (path coefficient), S.E (standard error), M and N (sample size of M and N groups)

Table 6 shows that the difference caused by the two subgroups is statistically significant in two paths (t = -5.698 and 6.039). With respect to the results obtained from the Smith-Satterthwaite test, the effects of privacy calculus on the variables were different depending on the frequency of the exercise group. Accordingly, hypothesis 9 was supported.

6. Discussion and Conclusion

In recent years, the issue of privacy information with respect to users of wearable devices has been constantly discussed, and studies were conducted in the early stages of wearable device development. Privacy concerns have focused on the identification of factors that affect users' acceptance of the devices [30]. Thus, this study verified the factors of information privacy concerns and the perceived values of users of wearable devices based on privacy calculus theory, and we investigated the relationship between the users' intention to disclose information and the continuance intention to use the wearable device from an integrated perspective. The implications of this study are as follows.

First, the privacy calculus results verified that both the users' perceived privacy concern and perceived values impacted their intention to disclose information, as argued in previous studies [3, 25, 33]. The perceived value had a greater impact than perceived privacy concern on information disclosure, and the perceived privacy concern decreased the perceived value from a wearable device user's perspective. This can be interpreted to mean that users are more likely to provide information through the device and use it continuously if the values provided by the device and services are perceived to be greater than existing privacy concerns in the field of wearable devices. All factors that affect the information privacy concerns and the perceived values of wearable device users proposed in this study were validated. Of the two variables that affect the perceived values, enjoyment had a large impact, which is in agreement with previous studies that indicate that compared with other factors, enjoyment and hedonic values had a greater impact on the acceptance of and satisfaction with the device [30, 31].

Perceived surveillance has a greater effect on the perceived privacy concern than secondary use of information. This result was affected by the properties of the wearable device and its personalized service environment. As previously discussed, service providers of connected devices are able to use technologically advanced surveillance means to track and monitor a user [18].

Second, the result involving the frequency of exercise comparison was as follows. It was found that factors affecting on perceived privacy concerns are significantly different. The low-exercise group had a concern about secondary use of information. This is similar to the result of a previous study, which revealed that users perceived risk owing to service provider actions [38]. This implies that users are concerned about improper information use by service providers, which does not involve technical surveillance or data leakage due to errors. In contrast, the variable of perceived surveillance was validated in the high-exercise group. It was shown that compared with the low-exercise group, the high-exercise group is more concerned about surveillance when using the device in situations where the exercise records of users are transmitted for a longer time, and when a wider variety of user data may be collected.

Theoretical implications of this study are as follows. We examined a more comprehensive privacy calculus model to understand concerns by individuals about information privacy pertaining to wearable devices. We applied variable adapting as applied in the MUIPC model, which reflects the mobility of mobile devices. This research is meaningful as it applies information disclosure to evaluate users' continuance intention to utilize the wearable device. We conducted a survey of an actual user group of wearable devices, where the intention to disclose information may be understood as the concept of continuous data sharing and synchronization. In addition, we identified that an individual's privacy calculus factor is different based on the frequency of exercise. Future research on wearable devices is required to better understand their service features and user context such as frequency of machine usage and service loyalty.

This research provides insights for service providers, enabling them to utilize better strategies and policies to address wearable-device privacy issues. First, users were concerned about surveillance by wearable devices, especially in the high-exercise group. We can deduce that if users with surveillance concerns may not use the synchronization functions of wearable devices. In order to collect customer data to establish business strategies, continuous data synchronization is very important. Therefore, operators should find ways of lowering customer privacy concerns. The low-exercise group is concerned about the secondary use of information, in terms of whether service providers use acquired data responsibly. This may have a negative impact on personal information disclosure and continued use in the future. Previous studies found that efforts by service providers to protect user privacy mitigated the privacy concerns of some users [54]. Therefore, when offering products and services, service providers of wearable devices should reassure users that there is no risk of exploitation of data collected via the device beyond the original intended purpose.

The limitations of this study are as follows. This study was conducted on undergraduate students who had the highest rate of using wearable devices. However, owing to the universality of wearable devices, it would also be useful to present the results of the privacy calculus on wearable devices for other age groups. In addition, exercise groups were divided by the mean exercise frequency of the entire sample. However, clearer evidences of group classification should be provided based on reviews of additional previous studies, and differences between groups should be verified using diverse criteria. Nevertheless, in this study, the difference between the groups was evident based on the privacy calculus according to the frequency of exercise, which is significant in this study, as it confirmed the importance

of exercise-related variables in the privacy issue of wearable devices. Future research should be conducted to verify the moderating effects of exercise variables. In addition, although the perceived value of wearable devices affects the intention to disclose information, privacy concerns also have an impact on the perceived value, and the intention to disclose information affects the continuance intention of using the device, which indicates the importance of adequate strategies in terms of privacy issue management to encourage continuous use of wearable devices. Comprehensive studies that focus on such concerns regarding information management should be conducted in the future.

References

[1] H. Li, J. Wu, Y. Gao, and Y. Shi, "Examining individuals' adoption of healthcare wearable devices: an empirical study from privacy calculus perspective," *Int. J. Med. Inform.*, vol. 88, no. 555, pp. 8–17, 2016. Article (CrossRef Link)

[2] Y. Jang, "'Wearable era' health information leakage risk," *The Kyunghyang Shinmun*, 28-Feb-2017.

[3] T. Wang, T. D. Duong, and C. C. Chen, "Intention to disclose personal information via mobile applications: A privacy calculus perspective," *Int. J. Inf. Manage.*, vol. 36, no. 4, pp. 531–542, 2016. Article (CrossRef Link)

[4] K. Barnes, V. Kauffman, and C. Connolly, "Health wearables : early days," 2014.

[5] D. Yadron, "America's top privacy regulator refuses to wear a Fitbit," *The Guardian*, 2016.

[6] Z. Whittaker, "How Strava's 'anonymized' fitness tracking data spilled government secrets," *ZD net*, 2018.

[7] Y. Gao, H. Li, and Y. Luo, "An empirical study of wearable technology acceptance in healthcare," *Ind. Manag. Data Syst.*, vol. 115, no. 9, pp. 1704–1723, 2015. Article (CrossRef Link)

[8] M. Shin and Y. Lee, "A sutdy on the influential factors of purchase intention of wrist wearable device," *J. Korea Contents Assoc.*, vol. 15, no. 15, pp. 498–506, 2015. Article (CrossRef Link)

[9] S. Lee, W. Yoo, H. Park, and S. Kim, "An empirical study on acceptance intention towards healthcare wearable device," *J. Inf. Syst.*, vol. 25, no. 2, pp. 27–50, Jun. 2016. Article (CrossRef Link)

[10] H.-J. Son, S.-W. Lee, and M.-H. Cho, "Influential factors of college students' intention to use wearable device: an application of the UTAUT2 model," *J. Commun. Inf.*, vol. 68, pp. 7–33, 2014.

[11] M. Baek, H. Choi, and H. Lee, "Age-specific acceptance intention over wearable smart healthcare device," *Korean Jouranl Bus. Adm.*, vol. 28, no. 12, pp. 3171–3189, 2015. Article (CrossRef Link)

[12] N. Farag Awad and M. S. Krishnan, "The Personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Q.*, vol. 30, no. 1, pp. 13–28, 2006. Article (CrossRef Link)

[13] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information privacy: measuring individuals' concerns about organizational practices about organizational practices1," *MIS Q.*, vol. 20, no. 2, pp. 167–196, 1996. Article (CrossRef Link)

[14] K. A. Stewart and A. H. Segars, "An empirical examination of the concern for information privacy instrument," *Inf. Syst. Res.*, vol. 13, no. 1, pp. 36–49, 2002. Article (CrossRef Link)

[15] N. K. Malhotra, S. S. Kim, J. Agarwal, G. Tech, and W. Peachtree, "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model," *Inf. Syst. Res.*, vol. 15, no. 4, pp. 336–355, 2004. Article (CrossRef Link)

[16] M. J. Keith, S. C. Thompson, J. Hale, P. B. Lowry, and C. Greer, "Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior," *Int. J. Hum. Comput. Stud.*, vol. 71, no. 12, pp. 1163–1173, 2013. Article (CrossRef Link)

[17] H. Chen and W. Li, "Mobile device users' privacy security assurance behavior: a technology threat avoidance perspective," *Inf. Comput. Secur.*, vol. 25, no. 3, pp. 330–344, 2017. Article (CrossRef Link)

[18] H. Xu, S. Gupta, B. Rosson, Mary, and M. Carroll, John, "Measuring mobile users' concerns for information privacy," in *Proc. of Proceedings of the 33rd International Conference on Information Systems*, 2012, no. June, pp. 1–16.

[19] H. J. Smith, T. Dinev, and H. Xu, "Inforamtion privacy research : an interdisciplinary review," *MIS Q.*, vol. 35, no. 4, pp. 989–1015, 2011. Article (CrossRef Link)

[20] R. S. Laufer and M. Wolfe, "Privacy as a concept and a social issue: a multidimensional developmental theory," *J. Soc. Issues*, vol. 33, no. 3, pp. 22–42, 1977. Article (CrossRef Link)

[21] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation," *Organ. Sci.*, vol. 10, no. 1, pp. 104–115, 1999. Article (CrossRef Link)

[22] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, 2006. Article (CrossRef Link)

[23] K.A. Park, "The effect of perceived value and information disclosure on continuous usage in location based services users," *Graduate School of Chosun University*, 2013.

[24] H. Xu, X. Luo, J. M. Carroll, and M. B. Rosson, "The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing," *Decis. Support Syst.*, vol. 51, no. 1, pp. 42–52, 2011. Article (CrossRef Link)

[25] J. Kim and S. Kim, "The effect of relationships between justice and privacy calculus on intention to disclose personal information," *J. Internet Electron. Commer. Res.*, vol. 14, no. 1, pp. 45–67, 2014.

[26] Y. Li, "Theories in online information privacy research: a critical review and an integrated framework," *Decis. Support Syst.*, vol. 54, no. 1, pp. 471–481, 2012. Article (CrossRef Link)

[27] I. Ajzen and M. Fishbein, *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, New Jersey: Prentice-Hall, 1980.

[28] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, Dec. 1991. Article (CrossRef Link)

[29] S. Kokolakis, "Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon," *Comput. Secur.*, vol. 64, pp. 122–134, 2017. Article (CrossRef Link)

[30] S. Chae, Y. Lee, Y. Jung, and S. M. Choi, "An investigation of users' intention to use wearable devices in the privacy-calculus framework," *Inf. Soc. Media*, vol. 17, no. 2, pp. 99–128, 2016.

[31] H. Kim, H. C. Chan, and S. Gupta, "Value-based adoption of mobile internet : an empirical investigation," *Decis. Support Syst.*, vol. 43, pp. 111–126, 2007. Article (CrossRef Link)

[32] S. Chen and C. Lin, "The impact of customer experience and perceived value on sustainable social relationship in blogs : an empirical study," *Technol. Forecast. Soc. Chang.*, vol. 96, pp. 40–50, 2015. Article (CrossRef Link)

[33] C. Morosan and A. DeFranco, "Disclosing personal information via hotel apps: a privacy calculus perspective," *Int. J. Hosp. Manag.*, vol. 47, pp. 120–130, 2015. Article (CrossRef Link)

[34] A. Weinhard and M. Hauser, "Explaining adoption of pervasive retail systems with a model based on UTAUT2 and the extended privacy calculus," in *Proc. of Twenty First Pacific Asia Conference on Information System(PACIS) 2017 Proceedings*, 2017, no. 217.

[35] H. Yang, J. Yu, H. Zo, and M. Choi, "User acceptance of wearable devices: an extended perspective of perceived value," *Telemat. Informatics*, vol. 33, no. 2, pp. 256–269, 2016. Article (CrossRef Link)

[36] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: a comparison of two theoretical models," *Manage. Sci.*, vol. 35, no. 8, pp. 982–1003, Aug. 1989. Article (CrossRef Link)

[37] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, vol. 13, no. 3, p. 319–340., 1989. Article (CrossRef Link)

[38] J. Bae, Y. Jung, and W. Cho, "Users' Privacy Concerns in the Internet of Things (IoT): The Case of Activity Trackers," *Knowl. Manag. Soc. Korea*, vol. 16, no. 3, pp. 23–40, 2015. http://dx.doi.org/10.15813/kmr.2015.16.3.002

[39] D. J. Solove, "A Taxonomy of Privacy," *Univ. PA. Law Rev.*, vol. 154, no. 3, pp. 477–564, 2006.

[40] M. J. Culnan and R. J. Bies, "Consumer privacy: balancing economic and justice considerations," *J. Soc. Issues*, vol. 59, no. 2, pp. 323–342, Jun. 2003. Article (CrossRef Link)

[41] F. V. Cespedes and H. J. Smith, "Database Marketing : New Rules for Policy and Practice," *Sloan Manag. Rev.*, vol. 34, no. 4, pp. 7–10, 1993.

[42] M. J. Dutta-Bergman, "Primary sources of health information: comparisons in the domain of health attitudes, health cognitions, and health behaviors," *Health Commun.*, vol. 16, no. 3, pp. 273–288, Jul. 2004. Article (CrossRef Link)

[43] H. K. Kim and Y. S. Kim, "The effects of smartphone application to increase physical activity among university students," *Korean J. Phys. Educ.*, vol. 51, no. 5, pp. 457–466, 2012.

[44] H. J. Kong, J. Kim, E. J. Hwang, J. Hong, and S. W. Kim, "Effects of healthcare smart home exercise program on the metabolic syndrome risk factors of obese elderly women," *J. Korean Gerontol. Soc.*, vol. 34, no. 1, pp. 103–114, 2014.

[45] V. G. Motti and K. Caine, "Users' privacy concerns about wearables," *Financial Cryptography and Data Security*, 2015, pp. 231–244.

[46] P. M. Bentler, "Comparative fit indexes in structural models.," *Psychol. Bull.*, vol. 107, no. 2, pp. 238–246, 1990. Article (CrossRef Link)

[47] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, and R. L. Tatham, *Multivariate data analysis. Uppersaddle River*. Prentice-Hall International, 1998.

[48] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information privacy concerns : linking individual perceptions with institutional privacy assurances," *J. Assoc. Inf. Syst.*, vol. 12, no. 12, pp. 798–824, 2011. Article (CrossRef Link)

[49] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies," *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879–903, 2003. Article (CrossRef Link)

[50] J. W. Kim, M. G. Kim, and S. H. Hong, *Writing paper with structural equation model*. Seoul: Communication Books, 2009.

[51] J. C. Anderson and D. W. Gerbing, "Structural equation modeling in practice: a review and recommended two-step approach.," *Psychol. Bull.*, vol. 103, no. 3, pp. 411–423, 1988. Article (CrossRef Link)

[52] Y. joon Cheon, S. K. Choi, J. Kim, and K. T. Kwak, "Antecedents of relational inertia and information sharing in SNS usage: the moderating role of structural autonomy," *Technol. Forecast. Soc. Change*, vol. 95, pp. 32–47, 2015. Article (CrossRef Link)

[53] W. Chin, "The partial least squares approach to structural equation modeling," *Mod. methods Bus. Res.*, vol. 295, no. 2, pp. 295–336, 1998.

[54] H. Xu and H.-H. Teo, "Alleviating consumers' privacy concerns in location-based services: a psychological control perspective," in *Proc. of Twenty-Fifth Int. Conf. Inf. Syst. ICIS 2004*, no. Beinat 2001, pp. 793–806, 2004.

Ji Yeon Cho is in Ph.D course at the Graduate School of Information and a researcher at Communications Policy Research Center in Yonsei University. She received her M.S. degree in Information System from Yonsei University in 2010. Her research interests include Big data service and policy, IoT Service and strategy.

Dr. Daesun Ko received his Ph.D in Sport and Leisure Studies from Yonsei University, Korea in 2007. He received his M.S. degree in Physical Education from Yonsei University in 2001. He is currently a lecturer in Department of Sport and Leisure Studies in Yonsei University. His research interests include mobile & sport.

Dr. Bong Gyou Lee is a Vice President/CIO and professor at Graduate School of Information in Yonsei University. He also has served as a director of Communications Policy Research Center since 2009. Dr. Lee received a B.A. from the Department of Economics at Yonsei University and he is also received his M.S. and Ph.D. from Cornell University. He was a Commissioner of the Korea Communications Commission in 2007 and 2008.