# Do IoT users trade off their information privacy?

Jungjoo Oh
Dankook University
winteroot@gmail.com

Soonbeom Kwon
Dankook University
kwonsb777@naver.com

Hwansoo Lee
Dankook University
hanslee992@gmail.com

## Abstract

*The advent of the Internet of Things (IoT) has not only improved people's quality of life but also raised concerns about information privacy. Although several studies have been conducted regarding information privacy concerns, there has not been sufficient discussion of the information privacy trade-off behavior in the IoT environment. Because previous studies only indirectly measured the information privacy trade-off behavior, the understanding of the behavior itself or its cause is limited. To address this issue, this study explored information privacy trade-off behavior in more depth using a large-scale sample and two-step analysis. Both panel data (23,724 samples for three years) and cross-sectional data (350 samples) were used in the analysis. The analysis results confirmed the existence of the information privacy trade-off for IoT users. Furthermore, it was found that the trade-off is associated with the social value of IoT devices and that men with IoT experience predominantly have strong trade-off behavior.*

**Keywords:** Internet of Things (IoT), information privacy trade-off, information privacy concerns, privacy calculus theory, perceived value.

## 1. Introduction

The Internet of Things (IoT) environment is a new growth engine that could lead the future industry by providing various convenient services at any time and in any place, without restrictions, through devices connected through the Internet [1, 2]. Although the rapidly popularized IoT environment is swiftly increasing quality of life by facilitating the generation and sharing of an increasing amount and variety of information, privacy infringement owing to the abuse of personal information is becoming a serious social issue [3]. The fact that the majority of popular IoT devices, such as internet protocol (IP) cameras, smart cars, and smart TVs, are vulnerable to security attacks, adds to security and privacy concerns [4].

Despite concerns as to privacy breaches, the diffusion of IoT devices has steadily progressed, and there remains a lack of understanding as to this paradoxical phenomenon. Several studies have been conducted on the leading factors affecting information privacy concerns within the IoT environment [5, 6]. They have mainly reported that information privacy concerns have an important impact on IoT device adoption and have proposed methods to decrease the concerns for the diffusion of IoT services. The proposals are primarily based on traditional privacy calculus theory [7], which states that lowering privacy concerns will result in users accepting IoT services. However, they have limitations in explaining the paradoxical attitude of users who want to use IoT services, even though privacy concerns are still high.

Existing privacy theories have presented a new perspective on the relationship between information privacy concerns and behavior. According to the privacy paradox perspective, consistency of attitude and behavior does not exist, but rather the relationship between these two factors differs from that which would be expected. Users are concerned about their privacy but do not act to protect it, or exchange their privacy and benefits [8]. These trade-off behaviors may be explained by various social psychological theories (e.g., protection motivation theory, social exchange theory), which are presented more frequently in the current general information technology environment. However, there are few studies on privacy trade-off behavior in the IoT environment. Furthermore, although previous studies have suggested that privacy behaviors may vary according to individual characteristics [9, 10], the relationship between privacy trade-off and personal characteristics in the IoT environment has not yet been sufficiently examined.

According to the privacy calculus theory [7], the benefits users receive are the key to sacrificing privacy, however, there is insufficient academic research concerning these factors. Existing studies do not clearly explain which benefits specifically lead to the trade-off in individual privacy. Thus, this study aimed to determine whether people have information privacy concerns in the IoT environment and whether there is a trade-off behavior despite these concerns. Additionally, this study examines how users' personal characteristics influence their trade-off behaviors in the IoT environment. Moreover, it discusses the complexity and

URI: https://hdl.handle.net/10125/103143
978-0-9981331-6-4

dynamic characteristics of information privacy concerns.

## 2. Theoretical Background

### 2.1. IoT Environment and Information Privacy

The IoT comprises various physical entities, including humans and the natural environment, connected to the Internet [11]. In the IoT, everything is connected, which means that all data are shared and centralized [12]. This increases the efficiency of work and convenience of living, but has the risk of sensitive information being leaked, which increases with the number of IoT devices connected to a network.

In the IoT environment, sensitive information is generated and collected, and users' lifestyle patterns can be easily monitored, which can lead to privacy issues [13]. Additionally, combining and analyzing the collected big data makes it possible to predict sensitive information (e.g., habits, wealth, and location). For example, closed-circuit television cameras (CCTV), temperature sensors, smart meters, and management applications related to smart home services can be hacked, increasing the risk of personal information leakage and privacy infringement [14, 15]. Although privacy breaches and security risks in the IoT environment are increasing, the market continues to grow. This paradoxical situation shows that IoT device users trade off their privacy and security to use new IoT services [16].

People recognize that their privacy is infringed upon when their information is collected or unintentionally predicted [17]. Privacy is a complex concept that is defined and recognized differently depending on discipline, country, culture, individual, and situation. Discussions on privacy have been conducted across various disciplines, including humanities, social sciences, and engineering. However, owing to differences in perspective and approach to privacy, there is no agreed definition, and the concept is differentiated according to the research field or purpose of the study [18].

According to existing research, privacy is classified into four types: physical, interactional, psychological, and informational [19, 20]. Among these, information privacy refers to the right to make decisions about one's own information [18, 21]. With the recent evolution of big data analysis, the privacy infringement of individuals is further increasing [22].

Early studies related to information privacy focused on defining concepts or measurement methods. Subsequently, various studies began highlighting behavioral changes that could be expressed as related to information privacy concerns. In the IoT environment, privacy violation is not limited to information leakage or privacy infringement, but also to remote control of other users' devices, which may also result in more serious forms of infringement, such as physical privacy invasion or physical damage. Privacy risk refers to the potential risk that users are subject to by providing personal information on the Internet [23]. In particular, people who have a high awareness of privacy risks or who have previously experienced infringement are more concerned about privacy violations. This tendency is a factor that determines the provision of personal information, and actions taken against the information collectors. If the levels of privacy concern increase, people could become reluctant to purchase or use IoT devices, thus suppressing IoT service acceptance [24].

### 2.2. Information Privacy Theory

The influence of the Internet has increased interest in information privacy, and theories that approach privacy attitudes and behavior from new perspectives have been proposed. As mentioned above, privacy calculus theory describes decision-making in relation to the provision of personal information [7]. According to this theory, information privacy is explained as an exchangeable means by which individuals gain benefits by providing information. In other words, this perspective looks at privacy from the perspective of commodities, in a departure from absolute legal rights. For example, when a company requests personal information from a consumer, the consumer goes through a calculation process that evaluates the benefits and risks of providing this personal information [25]. At this time, if the perceived benefit to the consumer is greater than or at least balanced by the risk, the consumer will provide personal information. This theory well explains the behavior related to privacy concerns, and so many studies have adopted this approach to expand the discussion of privacy.

Privacy studies have previously been conducted based on privacy concerns and behavioral outcomes. Recent studies suggest, however, that these relationships are not consistent, but rather that these are reversed or different, depending on the situation [18]. According to the privacy paradox theory [26], people tend to exhibit unique behaviors that do not correspond to the protection of their privacy, even when their privacy concerns are high, such as still providing personal information for small benefits. This privacy paradox results from the fact that consumers are obliged to provide personal information to use a specific service or to give up their privacy to use the service, even if their personal information is infringed [8]. These paradoxical behaviors are similar to the decision-making behavior proposed by privacy calculus theory, but differ in that

privacy paradox theory also explains the causes of irrational decision-making.

The complexity of privacy behavior can be found in several previous theories. Altman (1975) defined privacy as the selective control of access to the self. He emphasized the dialectical and dynamic nature of privacy, without viewing privacy from a passive perspective. He proposed that privacy regulation is a process of adjusting a spectrum of opening and closing to suit one's situation, and optimizing its boundaries. Petronio (2007) proposed the Communication Privacy Management (CPM) theory based on the dynamic properties of privacy. According to this theory, people have privacy boundaries for privacy breach decisions, and these boundaries are flexible depending on the context or situation. These boundaries may be individual or collective and are influenced by a variety of factors, including culture, sex, and motivation.

Zhou and Piramuthu (2015) proposed a contextual privacy theory that describes the multidimensional nature and conceptual dynamics of privacy. They presented a model that describes how consumers judge privacy violations based on three contextual factors (situation, place, and time) in the IoT environment. For example, even if the same sensitive information is provided, the privacy boundaries may vary depending on these contextual factors (medical situation vs. general situation). It also shows that the criteria for judging whether users' privacy has been infringed may differ depending on spatial or temporal characteristics. Because the IoT environment is also an environment that contains various contextual features, levels of privacy concerns may differ, and observing these boundary levels can help providers to understand IoT device user behavior.

## 2.3. Information Privacy Trade-off

Barnes (2006) discussed the paradoxical behaviors of individuals who provide personal information in spite of high privacy concerns in the social networking services (SNS) environment. Norberg et al. (2007) conducted an experimental study that verified the privacy paradox theory and found that these behaviors of people exist.

The privacy paradox behavior has many causes. Firstly, people are not exactly aware of the privacy risks [31, 32]. They behave irrationally, and privacy-protection behavior is not exhibited because they underestimate the magnitude of the risks of providing personal information. Secondly, forgetting about privacy risks also contributes to paradoxical behavior [33]. Rewards for providing personal information motivate the provision of information and work as a trigger for helping the user to forget about any associated risks. Thirdly, paradoxical behavior is also related to probability-based decision-making processes. In general, people place a higher value on the present than on the future, so they prefer to focus on clear immediate rewards rather than uncertain risks arising from the provision of personal information. People take on paradoxical behavior because of the uncertainty of the related risks [34]. Finally, the relationship with the information collector also causes paradoxical behavior. Trust of the collector tends to reduce a user's perception of the involved privacy risk [23]. In fact, these factors can all be explained by the trade-off behavior involved in privacy calculations. People decide whether or not to provide their personal information using limited knowledge based on a variety of factors, and paradoxical behavior occurs because this calculation process is irrational or subjective.

A high level of information privacy concern has a negative impact on the intention to use online services and provide information [33], while the perception of a high level of potential benefits leads to a willingness to provide personal information [35]. As providers can compensate for information privacy concerns by providing benefits such as usefulness or monetary compensation [36], several studies have been conducted on the calculation of information privacy and trade conditions. For example, JK Kim and Kim (2014) analyzed influential factors related to the intention of smartphone location-based service users to provide information, based on fairness theory and privacy calculus theory. For the users, privacy benefits have a stronger influence on the intention of privacy provision than privacy risks. Hann, Hui, Lee, and Png (2002) suggested that the intention to provide personal information to a website may be affected by financial rewards and convenience. Zhao, Lu, and Gupta (2012) analyzed the factors that influence the intention to disclose location-based information in location-based social network services. It was found that the extrinsic benefit of personalization and the intrinsic benefit of connectedness have a positive impact on the intention to disclose location-based information, whereas privacy concerns negatively affect the intention to disclose the location. The provision of incentives has a positive effect on external benefits, and the promotion of interactions has a positive effect on intrinsic benefits [39]. In addition, Derikx et al. (2015) studied trade conditions related to the privacy concerns of car owners in connection with IoT-enabled connected automobile services, suggesting that concerns about privacy in usage-based insurance services can be compensated using monetary benefits.

### 2.4. Perceived Value for the Information Privacy Trade-off

Perceived value refers to the value that customers perceive from a product or service [40]. Early studies on perceived value mainly defined it as a single dimension that is formed by the trade-off between loss and utility. Zeithaml (1988) defined perceived value as the perceived result of the benefits a customer obtains by spending time and money when purchasing a product. According to Bolton and Drew (1991), it is an overall evaluation of the products and services provided compared to the price paid. Woodruff (1997) defined it as customer evaluation and perceived preference for products and services. These studies analyzed perceived value from an economic perspective, but this approach had limitations because it could only grasp a fragmentary aspect of the perceived value compared to the diversity of the concept [43]. However, later studies considered perceived value as a multidimensional factor because it can be recognized differently depending on individuals or situations, and thus is a comprehensive concept [44].

Sweeney and Soutar (2001) argued that perceived value is formed by emotional, social (enhancement of social self-concept), functional (economic), and functional (performance) values. Ha and Jang (2010) divided it into hedonic and utilitarian values, whereas Chen and Hu (2010) classified it into symbolic and functional values. Since then, many researchers have attempted to define perceived value by dividing it into several dimensions, but it is not significantly far from the four dimensions suggested by Sweeney and Soutar (2001).

The perceived value theory has been used to analyze customers' perceived value in IoT research. Several studies have analyzed the impact of perceived value on IoT acceptance and usage intention [48, 49]. With regard to IoT device adoption, J.-C. Hong, Lin, and Hsieh (2017) measured the perceived value with hedonic and utilitarian values and found that these values have a significant impact on the user's intention to continue using smart watches in the future. Moreover, Hsiao and Chen (2018) categorized perceived value into four dimensions following Sweeney and Soutar (2001)'s approach and verified its relationship with smart watch purchase intention. The research results confirmed that emotional and economic values had a significant impact on the purchase intention of smart watches. Liu and Li (2018) also defined perceived value as Sweeney and Soutar (2001)'s four dimensions, among which social and emotional values play an important role in smart city adoption. Additionally, later studies discussed the acceptance and purchase behavior of various IoT-related devices, such as smart homes [53] and smart cars [54], based on the perceived value theory.

As the information privacy trade-off is a process of exchanging risk for value, the perceived value theory is a useful framework for understanding the kind of value for which people trade off their privacy. Studies have shown that the four sub-factors of Sweeney and Soutar (2001) can be useful for explaining the value of IoT devices. IoT devices enable users to use and manage their devices remotely, anytime, and anywhere. Furthermore, IoT devices have the economic advantage of reducing the time and effort required by using them remotely and can also contribute to the formation of consensus through exchanges between users. Therefore, in this study, the value that users can expect in the IoT environment is divided into functional, emotional, social, and monetary values based on the perceived value theory.

## 3. Research Procedure and Method

### 3.1. Research Procedure

As shown in Table 1, the research procedure was divided into two steps that examined the information privacy trade-off behavior of IoT device users. In Study 1, panel data of approximately 8,000 samples were used to examine changes in information privacy concerns over three years and determine whether there were statistically significant differences in their level of concern depending on whether they had IoT devices.

Because Study 1 is only able to indirectly verify trade-off behavior based on a large sample, further analysis is required. In Study 2, we directly measured the trade-off behaviors of IoT device users and determined which value factors influence the trade-off behaviors and which groups exhibit strong behaviors. The detailed analysis procedure is shown in Table 1.

**Table 1. Research design**

| | Study 1 | Study 2 |
|---|---|---|
| Objective | Confirmation of the IoT device users' trade-off behavior | Verification of what value and who trades off |
| Data Type | Panel data (2019~2021) | Cross-sectional data (2022) |
| Data Source | Korea Media Panel Data (www.kisdi.re.kr) | Online Survey (First data) |
| Number of samples | 2019: N = 7,892<br>2020: N = 7,788<br>2021: N = 8,044 | N = 350 |
| Method | Independent T-test | PLS-SEM |

## 3.2. Research Method and Data

**Study 1:** Study 1 used the information privacy concerns (IPCs) responses provided by the Korea Information Society Development Institute (KISDI) in the Korea Media Panel Survey to compare the IPC of those with and without IoT devices. The data in this panel included media use behavior of approximately 10,000 samples from the year 2010 to 2021, which is useful for both longitudinal and cross-sectional studies requiring a large sample size [18].

The data also included eight items (5-point Likert scale) regarding IPCs, which are based on Buchanan, Paine, Joinson, and Reips (2007). The measurement items included "I am concerned about submitting information on the Internet because of what others might do with it" and "I am concerned that my personal information may have been left on my previous digital devices."

From the data in this panel, the present study used data from 2019 to 2021. In this study, 7,892 samples from 2019; 7,788 from 2020; and 8,044 from 2021 were used, excluding respondents under the age of 20 years and those who did not respond to the IPC items (Table 2). The differences in IPC levels between the group with and without IoT devices were determined using a t-test.

**Table 2. Study 1 data**

| Category | | 2019 N (%) | 2020 N (%) | 2021 N (%) |
|---|---|---|---|---|
| Gender | Male | 3708(47.0) | 3666(47.1) | 3757(46.7) |
| | Female | 4184(53.0) | 4122(52.9) | 4287(53.3) |
| Age | 20~29 | 1214(15.4) | 1214(15.6) | 1271(15.8) |
| | 30~39 | 1023(13.0) | 894(11.5) | 843(10.5) |
| | 40~49 | 1931(24.5) | 1796(23.1) | 1731(21.5) |
| | 50~ | 3724(47.1) | 3884(49.8) | 4199(52.2) |
| Educational Background | High Sc. | 1136(14.4) | 1166(15.0) | 1265(15.7) |
| | Under. | 2920(37.0) | 2812(36.1) | 2853(35.5) |
| | Grad. | 3836(48.6) | 3810(48.9) | 3926(48.8) |
| Monthly Income (Korean Billion Won) | < 1 | 2891(36.6) | 2812(36.1) | 2944(36.6) |
| | 1~2 | 1715(21.7) | 1448(18.6) | 1268(15.8) |
| | 2~3 | 1817(23.0) | 1946(25.0) | 2008(25.0) |
| | 3~4 | 875(11.1) | 947(12.2) | 1101(13.7) |
| | 4 < | 594(7.5) | 635(8.1) | 723(8.9) |
| IoT Device Possession | Yes | 290(3.7) | 317(4.1) | 499(6.2) |
| | No | 7602(96.3) | 7471(95.9) | 7545(93.8) |
| Total | | 7892 | 7788 | 8044 |

**Study 2:** In Study 2, the Partial Least Squares Structural Equation Modeling (PLS-SEM) technique was applied to examine the relationship between the four perceived value factors of the study by Sweeney and Soutar (2001) and Information Privacy Trade-off Behavior (IPTB). The IPTB items were developed based on Dinev and Hart (2006). The items in Study 2 were measured on a 7-point Likert scale. Table 3 shows the measurement items used in Study 2.

**Table 3. Measurement items of study 2**

| Construct | | Items |
|---|---|---|
| Functional Value | FUV1 | is well made. |
| | FUV2 | has consistent quality. |
| | FUV3 | provides convenient functions. |
| Economic Value | ECV1 | is reasonably priced. |
| | ECV2 | offers value for money. |
| | ECV3 | would be economical. |
| Social Value | SOV1 | would make a good impression on others. |
| | SOV2 | would improve the way I am perceived. |
| | SOV3 | is something people around me recommend. |
| Emotional Value | EMV1 | is the one I would enjoy. |
| | EMV2 | is interesting. |
| | EMV3 | would please me. |
| Information Privacy Trade-off Behavior (Dependent Variable) | IPTB1 | It is acceptable to provide personal information to use the IoT devices. |
| | IPTB2 | Experiencing privacy concerns is acceptable when using IoT devices. |
| | IPTB3 | Even with information privacy concerns, using the IoT devices is worthwhile. |
| | IPTB4 | I will continue to use IoT devices despite information privacy concerns. |

A professional survey company (www.opensurvey.com) in South Korea collected the research sample for Study 2. In December 2021, 350 respondents provided information on their experiences with IoT devices. To make the characteristics of the research sample similar to Study 1, only individuals aged 20 years or older were selected. Table 4 shows the demographic characteristics of the data.

**Table 4. Study 2 data**

| Category | | N (%) |
|---|---|---|
| Gender | Male | 175(50.0) |
| | Female | 175(50.0) |
| Age | 20~29 | 88(25.1) |
| | 30~39 | 88(25.1) |
| | 40~49 | 88(25.1) |
| | 50- | 86(24.6) |
| Educational Background | ~High school | 50(14.3) |
| | Undergraduate | 252(72.0) |
| | Graduate | 42(12.0) |
| | Else | 6(1.7) |
| Monthly Income (Korean Billion Won) | < 1 | 56(16.0) |
| | 1~2 | 36(10.3) |
| | 2~3 | 88(25.1) |
| | 3~4 | 70(20.0) |
| | 4 < | 100(28.6) |
| Total | | 350 |

## 4. Results

**Study 1:** Jamovi 2.25, a statistical software, was used in Study 1. The Cronbach's alpha value of IPC was verified to confirm the reliability of the response. The internal consistency of the measurement of the eight items of the IPC for Study 1 was confirmed with a value of 0.94 or greater over the three sampled years.

According to the results (Table 5), the IPC level of the entire sample from 2019 to 2021 was approximately 3.5. This indicates that respondents had few IPCs. The t-test confirmed that the IPC level of the group with IoT devices was statistically significantly higher than that of the other group. For those three years, the level of IPC in the group using IoT devices was high, at approximately 4. Despite the growing number of IoT users from 2019 to 2021 (Table 2), there was a continued difference in the IPC levels. This indicates that IoT device owners continue to use IoT devices despite high IPCs, which suggests that, indirectly, they trade off their information privacy when using IoT devices.

**Table 5. T-test results**

| Year | Mean (S.D) | Comparison based on the use of IoT devices | | | |
|---|---|---|---|---|---|
| | | Yes | No | T | P |
| 2019 | 3.57(0.91) | 3.92 | 3.56 | 6.51 | < 0.001 |
| 2020 | 3.62(0.98) | 4.02 | 3.61 | 7.39 | < 0.001 |
| 2021 | 3.42(1.07) | 3.85 | 3.39 | 9.21 | < 0.001 |

**Study 2:** In Study 2, the Smart PLS 3.0 software was used for PLS-SEM analysis. First, the reliability and validity of the research model of Study 2 were evaluated using confirmatory factor analysis. The measurement model was validated using Cronbach's α, rho_A, composite reliability (CR), and average variance extracted (AVE). To avoid non-convergent validity issues, Cronbach's α, CR, and rho_A should be above 0.7 and AVE should be greater than 0.5 [56]. Because the IPTB2 item had a relatively low loading value (0.66), it was removed from the measurement model for strict analysis. As shown in Table 6, it was confirmed that there were no problems with the reliability and convergent validity of the measurement model.

According to the mean values of the measurement items (Table 6), the respondents perceived the functional value of the IoT devices to be relatively high (mean = 5.13). Moreover, the economic value of the IoT devices was perceived to be relatively low (mean = 4.58). The IPC trade-off behavior of the respondents was at the neutral level (mean = 3.91).

**Table 6. Measurement model evaluation**

| Items | Mean | Loading | α | rho_A | CR | AVE |
|---|---|---|---|---|---|---|
| FUV1 | 5.01 | 0.92 | 0.89 | 0.89 | 0.93 | 0.81 |
| FUV2 | 5.08 | 0.91 | | | | |
| FUV3 | 5.31 | 0.88 | | | | |
| ECV1 | 4.51 | 0.88 | 0.84 | 0.85 | 0.90 | 0.76 |
| ECV2 | 4.85 | 0.87 | | | | |
| ECV3 | 4.37 | 0.86 | | | | |
| SOV1 | 4.69 | 0.88 | 0.85 | 0.85 | 0.91 | 0.77 |
| SOV2 | 4.41 | 0.90 | | | | |
| SOV3 | 4.74 | 0.85 | | | | |
| EMV1 | 4.69 | 0.91 | 0.90 | 0.91 | 0.94 | 0.83 |
| EMV2 | 4.99 | 0.92 | | | | |
| EMV3 | 4.88 | 0.91 | | | | |
| IPTB1 | 3.63 | 0.82 | 0.82 | 0.82 | 0.90 | 0.73 |
| IPTB3 | 3.88 | 0.88 | | | | |
| IPTB4 | 4.22 | 0.87 | | | | |

Discriminant validity was evaluated based on Fornell and Larcker (1981)'s method, which compares the square root value of each variable's AVE and heterotrait–monotrait ratio (HTMT). When the square root value of AVE does not exceed the diagonal correlation coefficient value and HTMT is less than 0.85, discriminant validity is assured. The results satisfied Fornell and Larcker (1981)'s criteria and the highest HTMT value was 0.79.

To verify the relationship between independent and dependent variables, the bootstrapping method (subsamples = 5000) was applied. The bootstrapping results indicated that economic, social, and emotional value constructs had a significant positive (+) effect on the IPTB. Among them, the social value was found to have a relatively strong influence on the trade-off behavior.

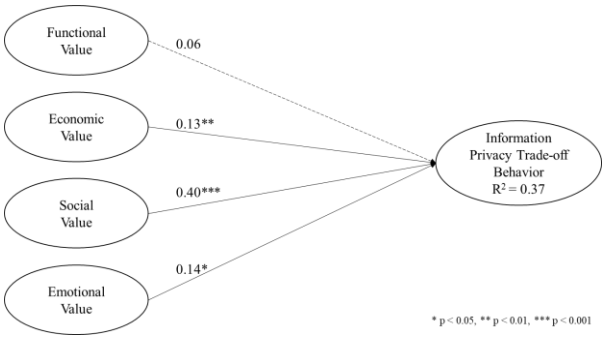


**Figure 1. PLS Results**

To determine which group exhibited a strong IPC trade-off behavior, regression analysis was also performed with demographic variables (gender, age, income level, educational background, and IoT device experiences) as independent variables. The results indicated that men have a statistically strong trade-off behavior (β = -0.15, p = 0.08), and although it did not

reach the significance level, the longer the experience of using IoT devices, the greater was the trade-off behavior ($\beta = 0.08$, $p = 0.17$).

# 5. Discussion

## 5.1. Findings

This study examined the IPTB of IoT device users. According to Study 1, IoT device owners have higher levels of IPCs than IoT device non-owners. Moreover, the level of concern of IoT device owners was high for the three years, which implies that the IoT users trade off their use of IoT devices despite the concerns. In general, a high level of information privacy concern may affect both the users' intention to use the product or service and their protective behavior [7, 33].

Despite the high level of IPCs associated with IoT devices, the fact that users possess and use IoT devices indicates that trade-off behavior exists. In other words, users accept the information privacy trade-off between the benefits of using IoT devices and their concerns regarding information privacy. Thus, it is confirmed that an IPTB exists in the IoT environment. This result is consistent with that of previous studies [8, 30] conducted on the privacy paradox phenomena.

Study 2 sought to determine who trade off privacy and why. Among the four value factors, social, emotional, and economic values were found to have a significant impact on trade-off behavior. In particular, the results indicate that social values play an important role. The results can be interpreted in two ways. To maximize the connectivity characteristics of IoT devices, a network effect is required. To achieve this, social awareness and demand for IoT devices are crucial; therefore, the impact of social value is important for the trade-off.

Another possible interpretation could be ascribed to the characteristics of the sample. As Asian cultures are characterized by strong collectivistic tendencies, an existing study [52] argued that social values play an important role in the IoT device adoption to improve quality of life. By contrast, functional values did not have a significant impact on the trade-off behavior, which may be because the IoT functions are related to the personalization paradox [57]. Because the advancement of IoT functions is highly correlated with personal information, it implies that the functional value may not affect the trade-off if information transparency or privacy protection is unclear according to the use of functions.

The trade-off behavior was found to be statistically significantly higher among men, and although statistical significance was not established, the experience of using IoT also had a positive effect. Trade-off behavior among men is higher than that of women because, in general, men have a more innovative and positive attitude towards technology adoption [58]. In addition, the high trade-off behavior of people with long experience in IoT can be attributed to cognitive experience, which lowers the privacy risk.

## 5.2. Contributions

One theoretical contribution of this study is that it confirms that even in the IoT environment, there is a trade-off phenomenon regarding the use of IoT devices despite privacy concerns. Previous studies examined privacy trade-off mainly in terms of Internet services, such as social network services; however, the existence of similar concepts in the new IoT information technology environment suggests a general change in user perception of privacy.

Unlike the Internet, IoT environments can cause serious damage if there is a security breach. A loss of control over IoT devices can cause serious privacy breaches, including physical or personal exposure. Despite these risks, the convenience of IoT devices makes them highly adapted to the needs of their users, so the trade-off tends to be strong. In addition, this study introduced an item for directly measuring the IPTB, and performed an empirical analysis to understand the trade-off phenomenon in more detail.

As a practical contribution, this study shows that IoT service providers should be aware that consumers have a high level of privacy concerns related to their use of IoT devices. Understanding the privacy concerns of users can help determine the direction in which an organization should develop to increase IoT device adoption. In particular, the strong trade-off tendency of highly experienced men shows the need for IoT service providers to develop products and services with these demographics in mind. Lowering privacy concerns for women and other groups who use IoT devices could be a good strategy for making IoT devices more pervasive.

## 5.3. Limitations and Further Study

This study demonstrated that the information privacy trade-off and paradox exist within the IoT environment and that IoT users display a trade-off tendency. Although the results are interesting and meaningful, this study can be improved. One limitation is that the analysis of the validation of IPTB measurement items is still lacking. In the study, the trade-off behavior was measured with the minimum number of items; thus, additional efforts should be made to develop a more reliable measurement item. Another limitation is that this study was conducted using self-reported data, despite its large sample size. This study

did not examine the differences in privacy trade-off associated with the different IoT devices in use. A broader and more integrated study might confirm the phenomena highlighted in this study while taking these other factors into account. Thus, further analysis and discussion should be conducted in future studies.

## Acknowledgment

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2018S1A5A8027174); and by the Growth Support Project for Industrial Innovation Talent of MOTIE (P0008703).

## References

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

[2] Park, H. & Rhee, S.-B. (2018). IoT-based smart building environment service for occupants' thermal comfort. *Journal of Sensors, 2018*.

[3] Aldrich, F. K. (2003). Smart homes: past, present and future *Inside the smart home* (pp. 17-39): Springer.

[4] Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review, 31*(5), 618-627.

[5] Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: an extension of the theory of planned behavior. *Industrial Management & Data Systems, 117*(1), 68-89.

[6] Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior, 92*, 273-281.

[7] Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research, 17*(1), 61-80.

[8] Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

[9] Lee, M.-N. & Shim, J.-W. (2009). The moderating effect by gender in the relationship between the perception of online privacy and use of privacy protection strategy. *Media, Gender and Culture, 12*, 166-190.

[10] Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389-418.

[11] Wang, Z., Ding, H., Han, J., & Zhao, J. (2013). Secure and efficient control transfer for IoT devices. *International Journal of Distributed Sensor Networks, 9*(11), 503404.

[12] Sung, G.-M., Shen, Y.-S., Hsieh, J.-H., & Chiu, Y.-K. (2019). Internet of Things–based smart home system using a virtualized cloud server and mobile phone app. *International Journal of Distributed Sensor Networks, 15*(9), 1550147719879354.

[13] Lee, H. (2020). Home IoT resistance: Extended privacy and vulnerability perspective. *Telematics and Informatics, 49*, 101377.

[14] Qu, Y., Yu, S., Zhou, W., Peng, S., Wang, G., & Xiao, K. (2018). Privacy of things: Emerging challenges and opportunities in wireless internet of things. *IEEE Wireless Communications, 25*(6), 91-97.

[15] Xu, R., Zeng, Q., Zhu, L., Chi, H., Du, X., & Guizani, M. (2019). Privacy leakage in smart homes and its mitigation: IFTTT as a case study. *IEEE Access, 7*, 63457-63471.

[16] Ziar, R. A., Omar, R., Ahmad, I., & Niazy, S. (2019). Information Privacy Paradox and Fatigue in IoT. *Technology, 1*(1), 37-46.

[17] Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security, 77*, 226-261.

[18] Lee, H., Wong, S. F., Oh, J., & Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Government Information Quarterly, 36*(2), 294-303.

[19] Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of social and personal relationships, 6*(2), 131-158.

[20] Lee, H., Lim, D., Kim, H., Zo, H., & Ciganek, A. P. (2015). Compensation paradox: the influence of monetary rewards on user behaviour. *Behaviour & Information Technology, 34*(1), 45-56.

[21] Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology, 68*(3), 459-468.

[22] Dinev, T. & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.

[23] Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly, 35*(3), 445-459.

[24] Yang, H., Lee, W., & Lee, H. (2018). IoT smart home adoption: the importance of proper level automation. *Journal of Sensors, 2018*.

[25] Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2019). e-Commerce Sustainability: The Case of Pinduoduo in China. *Sustainability, 11*(15), 4053.

[26] Hallam, C. & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior, 68*, 217-227.

[27] Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*: CA: Brooks/Cole Publishing.

[28] Petronio, S. (2007). Translational research endeavors and the practices of communication privacy

management. *Journal of Applied Communication Research, 35*(3), 218-222.
[29] Zhou, W. & Piramuthu, S. (2015). Information relevance model of customized privacy for IoT. *Journal of business ethics, 131*(1), 19-30.
[30] Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).
[31] LaRose, R. & Rifon, N. J. (2007). Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41*(1), 127-149.
[32] Milne, G. R. & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive marketing, 18*(3), 15-29.
[33] Bélanger, F. & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly, 35*(4), 1017-1042.
[34] Kim, J. & Kim, S. (2014). A Study on Privacy Paradox between Privacy Concern and Information Disclosure Behavior: Focus on Privacy Calculus Theory. *Entrue Journal of Information Technology, 13*(3), 139-152.
[35] Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.
[36] Derikx, S., de Reuver, M., Kroesen, M., & Bowman, H. (2015). *Buying-off privacy concerns for mobility services in the Internet-of-things era: A discrete choice experiment on the case of mobile insurance.* Paper presented at the Bled eConference.
[37] Kim, J. & Kim, S. (2014). The effect of relationships between justice and privacy calculus on intention to disclose personal information. *The Journal of Internet Electronic Commerce Research, 14*(1), 45-67.
[38] Hann, I.-H., Hui, K.-L., Lee, T., & Png, I. (2002). Online information privacy: Measuring the cost-benefit trade-off. *Twenty-Third International Conference on Information Systems*.
[39] Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce, 16*(4), 53-90.
[40] Bolton, R. N. & Drew, J. H. (1991). A longitudinal analysis of the impact of service changes on customer attitudes. *Journal of marketing, 55*(1), 1-9.
[41] Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence. *Journal of marketing, 52*(3), 2-22.
[42] Woodruff, R. B. (1997). Customer value: the next source for competitive advantage. *Journal of the academy of marketing science, 25*(2), 139-153.
[43] Al-Sabbahy, H. Z., Ekinci, Y., & Riley, M. (2004). An investigation of perceived value dimensions: implications for hospitality research. *Journal of travel research, 42*(3), 226-234.
[44] Petrick, J. F. (2002). Development of a multi-dimensional scale for measuring the perceived value of a service. *Journal of leisure research, 34*(2), 119-134.
[45] Sweeney, J. C. & Soutar, G. N. (2001). Consumer perceived value: The development of a multiple item scale. *Journal of retailing, 77*(2), 203-220.
[46] Ha, J. & Jang, S. S. (2010). Perceived values, satisfaction, and behavioral intentions: The role of familiarity in Korean restaurants. *International Journal of Hospitality Management, 29*(1), 2-13.
[47] Chen, P.-T. & Hu, H.-H. (2010). The effect of relational benefits on perceived value in relation to customer loyalty: An empirical study in the Australian coffee outlets industry. *International Journal of Hospitality Management, 29*(3), 405-412.
[48] Kim, Y., Park, Y., & Choi, J. (2017). A study on the adoption of IoT smart home service: using Value-based Adoption Model. *Total Quality Management & Business Excellence, 28*(9-10), 1149-1165.
[49] Hu, G., Chohan, S. R., & Liu, J. (2022). Does IoT service orchestration in public services enrich the citizens' perceived value of digital society? *Asian Journal of Technology Innovation, 30*(1), 217-243.
[50] Hong, J.-C., Lin, P.-H., & Hsieh, P.-C. (2017). The effect of consumer innovativeness on perceived value and continuance intention to use smartwatch. *Computers in Human Behavior, 67*, 264-272.
[51] Hsiao, K.-L. & Chen, C.-C. (2018). What drives smartwatch purchase intention? Perspectives from hardware, software, design, and value. *Telematics and Informatics, 35*(1), 103-113.
[52] Liu, C. & Li, D. (2018). *Impact of perceived value on smart city application.* Paper presented at the 2018 Chinese Control And Decision Conference (CCDC).
[53] Hong, A., Nam, C., & Kim, S. (2020). What will be the possible barriers to consumers' adoption of smart home services? *Telecommunications Policy, 44*(2), 101867.
[54] Park, J., Nam, C., & Kim, H.-j. (2019). Exploring the key services and players in the smart car market. *Telecommunications Policy, 43*(10), 101819.
[55] Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology, 58*(2), 157-165.
[56] Fornell, C. & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 18*(1), 39-50.
[57] Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems, 34*(2), 369-400.
[58] van Rijnsoever, F. J. & Donders, A. R. T. (2009). The effect of innovativeness on different levels of technology adoption. *Journal of the American society for information science and technology, 60*(5), 984-996.