sustainability

MDPI

Article

Investigating the Personalization–Privacy Paradox in Internet of Things (IoT) Based on Dual-Factor Theory: Moderating Effects of Type of IoT Service and User Value

Ae-Ri Lee

Department of Business Administration, Sangmyung University, Seoul 03016, Korea; sharon@smu.ac.kr

Abstract: Despite people's concerns over privacy leakage in the Internet of Things (IoT), the needs for personalized IoT services are increasing, creating a conflicting phenomenon viewed as the personalization–privacy (P–P) paradox. This study proposes a research model that utilizes dual-factor theory to investigate the P–P paradox in IoT. It aims to analyze the impact of the dual factor—personalization and privacy concerns related to IoT services—on the intention to use IoT. Further, the model includes four-dimensional motivated innovativeness and previous privacy-invasion experience as key antecedents of the dual factor. Particularly, this study examines the moderating effects of the type of IoT service and user value on the relationship between dual factor and usage intention. Data were collected using a web-based survey. The results showed that personalization had a significant impact on the intention to use IoT, whereas privacy concerns did not. The effects of all antecedents except social innovativeness were significant. The P–P paradox phenomenon appeared differently depending on the type of IoT service and user value. This study contributes to gaining a better understanding of the factors that influence the increase in IoT usage in terms of both protecting and appropriately using personal information for IoT services.

Keywords: Internet of Things; personalization–privacy paradox; dual-factor theory; IoT service type; IoT user value; motivated innovativeness

Citation: Lee, A.-R. Investigating the Personalization–Privacy Paradox in Internet of Things (IoT) Based on Dual-Factor Theory: Moderating Effects of Type of IoT Service and User Value. *Sustainability* **2021**, *13*, 10679. https://doi.org/10.3390/su131910679

Academic Editors: Sara Shirowzhan and Willie Tan

Received: 22 August 2021
Accepted: 24 September 2021
Published: 26 September 2021

1. Introduction

With the development of Internet of Things (IoT) technologies, our society is evolving into a hyper-connected society. In IoT environments, people and their surrounding objects are connected through sensors and communication networks to exchange information and interact, thus creating new value. By 2025, more than 75 billion objects, a nearly threefold increase from 2019, are expected to be connected [1], and the IoT market size is forecasted to increase to more than $1 trillion by 2030 [2]. IoT is expected to enhance human life and bring innovations to various industries.

In IoT environments, people find it difficult to recognize activities related to autonomously collecting, combining, and sharing data. In such IoT environments, analyzing the big data collected can provide a personalized context-aware service that is tailored to individual preferences and situations, thereby improving human convenience [3]. Conversely, as the amount and type of information newly collected in IoT increase exponentially, privacy invasion issues are emerging [4]. IoT allows personal information to be collected and used from a large number of devices. Compared to existing online services, this collection increases the quantity and types of information collected, including sensitive and detailed personal information, such as personal habits, tastes, and route of paths [5]. As IoT proliferates, data collected from diverse sources can be combined to facilitate personal profiling and tracking through data mining technologies. Thus, the risk of privacy violations might increase [6,7]. In fact, some privacy breaches have occurred because of IoT; examples include the unauthorized collection of personal information by telematics service providers, video leakages by home webcam manufacturers, hacking of baby

monitor services, personal information leakages using drones, and smart car hacking demonstrations [8,9].

Despite people's concerns over the leakage of personal information in the IoT environment, individuals' needs for personalized IoT services are increasing, creating a conflicting phenomenon viewed as the privacy paradox phenomenon [10]. A privacy paradox is a phenomenon wherein both negative and positive aspects of privacy coexist, and inconsistency is created between beliefs and behaviors about privacy—it is also referred to as the personalization–privacy paradox (P–P paradox) [11,12]. Acknowledging the importance of this phenomenon, scholars have recently investigated the impact of IoT services on usage behavior. However, extant research suffers from its partial approach to the phenomenon in that most research investigates only the positive aspects, for example, personalized services [13,14], whereas some research focuses on the negative side—for example, privacy concerns [5,7,9]. Privacy calculus theory asserts that consumers weigh the tradeoffs between the benefits of personalized services and the costs of privacy concerns [15]. When the perceived benefits exceed the perceived costs, consumers are willing to use IoT services, and vice versa. Therefore, considering these two factors simultaneously is important because the net effects of counteracting forces determine IoT service usage behavior.

Mitigating the weaknesses in this line of existing research, this study attempts to make three specific contributions: (1) consideration of both personalization and privacy concerns (P–P) factors based on the dual-factor theory [16,17]; (2) identification of the antecedents of personalization and those of privacy concerns; and (3) investigation of moderating effects based on the type of IoT service and user value concerning the relationship between P–P factors and usage behavior.

First, dual-factor theory is used as the overarching theory as it identifies two different types of influencers for information system (IS) usage behavior—that is, enablers and inhibitors—that work independently and simultaneously. Additionally, it provides a theoretical foundation that the two counteracting forces have different antecedents. This study investigates how the P–P paradox influences the intention to use IoT services.

Second, few studies have investigated the antecedents of either enablers or inhibitors of IoT service usage. This study extends its research design to include the antecedents of enablers and inhibitors. As user perceptions of personalization benefits (enablers) and privacy concerns (inhibitors) are formed through different routes, different theories are used to identify the antecedents. Regarding the former, the individual innovativeness theory is referenced to identify the four dimensions of innovativeness (cognitive, functional, hedonic, and social) following the existing research (e.g., [18–20]). Regarding the latter, existing studies about privacy concerns have identified previous privacy-invasion experience as the key antecedent (e.g., [6,10,21]). When an individual has a tendency of loss aversion, that is, weighing losses more heavily than gains, they tend to ensure that experienced loss does not occur again, thus increasing concerns about privacy protection [22]. Therefore, this study attempts to validate the applicability of these findings to the IoT service context.

Third, most research has been conducted in the context of a particular IoT device or service rather than encompassing multiple IoT services to compare the differences among them. However, a few recent studies (e.g., [23,24]) found that some IoT devices or services have a longer life span, whereas others (e.g., smart speakers) fade away after a short period of usage for some user groups. Garg [25], in a qualitative study on this phenomenon, elucidates the possibility that the reasons for using IoT services could vary depending on the type of IoT service and its value (e.g., IoT services for self-security in emergency, remotely controlling objects, and tracking and improving health and well-being). Accordingly, the relationship between the P–P tradeoff and use intention of IoT can be moderated by the type of IoT service and value.

In sum, this study focuses on the P–P paradox phenomenon in the IoT environment and endeavors to diagnose the phenomenon wherein a positive enabler and a negative inhibitor coexist in terms of both protecting and utilizing personal information from IoT services. Particularly, this study examines whether a positive enabler and a negative

inhibitor have different influences on the IoT use intention depending on the type of IoT service and user value. This study can contribute to gaining a more comprehensive understanding of the aspects that need more attention to increase individuals' willingness to use IoT services in the future. Furthermore, this study could serve to determine the aspects that should be emphasized more in certain services with a specific value to increase users' intention to continue to use IoT services. Ultimately, this study can provide strategic implications for the balanced development of IoT services and improvements to personalize these services through the appropriate use of personal information.

In Section 2, the conceptual background and a literature review are provided, and in Section 3, the research model and hypotheses are explained. Section 4 describes the research methodology, followed by a presentation of the data analysis and results. The final section concludes the study by discussing its contributions and implications.

2. Theoretical Background and Literature Review

This section is structured as follows. First, along with the description of the P–P paradox concept, the necessity of research on the IoT services usage from the P–P paradox perspective is explained, and the previous studies on the P–P paradox in the IS field performed so far are reviewed. Then, dual-factor theory, which is an overarching theory that is suitable for investigating the P–P paradox phenomenon in IoT, is introduced, and the conceptual framework of this study is presented based on this dual-factor theory. Thereafter, following the proposition that "enablers and inhibitors can have different antecedents" in the dual-factor theory, the antecedents of the P–P dual factor in this study are explained.

2.1. Personalization–Privacy Paradox in IoT

People have visions for using IoT services because of the convenience that interconnected services create, and people are provided with more customized services. Individuals are likely to constantly provide personal information in return for personalized services in order to gain various personalized benefits and tailored information from service providers [21]. However, people are also concerned about the negative consequences of excessive exposure of personal information and the possibility that this personal information will be collected indiscriminately and used inappropriately [26]. Existing studies have addressed concerns over the uncertainty regarding IoT services' invasion of user privacy [4,5]. Specifically, IoT services can store users' history related to sites visited, products purchased, and interest in certain services. Such data can be used as marketing information, thereby causing privacy concerns and infringement issues [6,7].

As such, people are concerned about the leakage of personal information but engage in conflicting behavior that reveals more personal information; this phenomenon is called the privacy paradox [27,28]. Using the privacy paradox perspective, Norberg et al. [27] argued that individuals might provide their personal information to obtain more benefits from using a particular service and experience anxiety over the exposure or secondary use of personal information that might arise accordingly. Recent studies have described the conflict between the need for personalization and the concern over personal privacy as the P–P paradox [12,15,29,30]. IoT services have the strength of a personalized service that uses personal information and offers the strong possibility of invading personal privacy [10]. Thus, diagnosing the current status of IoT service usage from the perspective of the P–P paradox is necessary to eventually provide strategic insights into the increasing of the use of IoT services.

Previous studies examined the P–P paradox in the IS field. Table 1 summarizes the literature review with the key results for research hypotheses. As shown in Table 1, some inconsistent findings about the analysis of the relationship between variables related to the paradox phenomenon exist in previous literature. Even if similar variables exist in the study models, the research contexts are different and the results can vary depending on moderating and mediating effects. For example, in Zhao et al. [21], both users'

privacy concerns (perceived costs) and personalization (perceived benefits) significantly influenced the intention to disclose location-related information for using location-based social networking service (SNS). However, in Kim et al. [4], perceived benefits affected the willingness to provide personal information when using IoT services, but perceived privacy risk did not matter. Barth et al. [11] studied mobile apps and found that privacy awareness and technical knowledge did not affect users' paradoxical behavior. Sheng et al. [31] revealed that the impact of personalization on the intention to adopt u-commerce services can be situation-dependent, such as during an emergency. These inconsistent findings in prior studies confirm the need for further investigations that consider the significant variables that can influence changes in the relationship of the P–P paradoxical variables in the research context.

Meanwhile, although IoT is an environment wherein the occurrence of the P–P paradox phenomenon is highly likely, very few studies have assessed this phenomenon in relation to IoT. Additionally, most existing IoT studies have examined the paradox for a specific IoT service [3,32,33]. There are various types of IoT services, and the phenomenon related to the P–P paradox could differ depending on the service and usage purpose [25,30]. Hence, this study attempts to investigate how the P–P paradox among IoT services appears differently by examining the moderating effects of the types of IoT services and users' value obtained through IoT services.

Regarding the background theory used in previous studies, most prior studies on the P–P paradox did not have a comprehensive theoretical foundation [11,29–31] or adopted privacy calculus theory [12,21,33], as shown in Table 1. The privacy calculus theory explains that consumers weigh the tradeoffs involved (e.g., between a personalized offering and privacy concerns); therefore, privacy calculus theory is useful and can be applied to paradox research. However, by introducing another theory, the P–P paradox phenomenon can be examined from a more comprehensive perspective. In this study, the dual-factor theory is employed as the overarching theory to investigate the P–P paradox phenomenon in IoT environments. The dual-factor theory could better explain the paradox phenomenon in the IS field because it supports the foundation that the enabler and inhibitor factors related to use intention in the IS can coexist independently. The dual-factor theory also provides a theoretical explanation for two paradoxical variables possibly having different antecedents. Therefore, the theory can be suitable as an overarching theory embracing the entire research model with two paradoxical factors—antecedents of the dual factor and use intention in the IoT context. The following subsection introduces the dual-factor theory in greater detail.

Table 1. Summary of previous literature on the P–P Paradox in IS.

Authors	Research Context	Theory	Key Findings
Aguirre et al. [29]	Digital media (e.g., display, search and social media)	–	The benefits of personalization may vary as a function of a medium through which communication is conveyed; personalization can enhance consumer engagement as well as diminish it by heightening privacy concerns.
Barth et al. [11]	Mobile phones apps	–	Neither technical knowledge nor privacy awareness impact on the paradoxical behavior in users; for selecting and downloading apps, privacy aspects do not play a significant role.
Guo et al. [30]	M-health	–	Perceived personalization and privacy concerns are positively and negatively associated with behavior intention; there are differences between age groups (youth vs. elderly).
Sheng et al. [31]	Ubiquitous commerce	–	The impacts of personalization on privacy concerns and adoption intention are situation dependent (higher during an emergency).

Table 1. *Cont.*

Authors	Research Context	Theory	Key Findings
Sutanto et al. [15]	Mobile advertising apps	Uses and Gratifications theory	P–P paradox can vary depending on users' gratifications.
Taddicken [28]	Social web	–	Privacy concerns impact self-disclosure, but different variables moderate this relation; social relevance and willingness positively influence self-disclosure, but the number of apps and age negatively influence self-disclosure.
Wang et al. [33]	Mobile apps	Privacy calculus theory	Self-presentation and personalized services positively influence perceived benefits, which in turn affect the intention to disclose personal information; perceived risks negatively affect the intention to disclose.
Xu et al. [12]	Location-awareness marketing (LAM)	Privacy calculus theory	The effects of personalization on privacy risk/benefit vary depending upon the type of personalization systems (covert > overt); previous privacy experience influences perceived risks of information disclosure; personal innovativeness influences the willingness to disclose personal information in LAM.
Zhao et al. [21]	Location-based SNS	Privacy calculus theory	Perceived cost (privacy concerns) and perceived benefits (personalization and connectedness) influence intention to disclose information; previous privacy invasions do not influence privacy concern; personal innovativeness influences intention to disclose personal information.
Kim et al. [4]	IoT	Privacy calculus theory	Perceived benefit affects the willingness to provide privacy information; perceived privacy risk does not matter.
Menard and Bott [6]	IoT	–	Privacy concerns positively affect risk beliefs and negatively affect trusting beliefs; prior experience with privacy violation negatively affects trusting beliefs.

2.2. Dual-Factor Theory

The dual-factor theory is based on Herzberg's motivation-hygiene theory or two-factor theory. Herzberg [34] identified that motivators—which drive job satisfaction in the work environment—and hygiene factors—which lead to job dissatisfaction—exist independently. The dual-factor theory was developed in the fields of IS with reference to Herzberg's motivation-hygiene theory [16]. In the dual-factor theory, the positive aspects of satisfaction are called "enablers", and the negative aspects of dissatisfaction are called "inhibitors". The dual-factor theory provides the following three propositions regarding the usage intention of IS [16,17].

First, the enabler and inhibitor factors can coexist and are not simply opposites of each other. The enablers and inhibitors can be distinguished from each other because the opposite concept of positiveness is not clear psychologically and does not necessarily mean negative if not positive. In other words, "inhibitors are more than just the antipoles of enablers and so are distinct constructs worthy of their own investigation" [17] (p. 808). People can simultaneously hold the perceptions of both inhibitors and enablers. Particularly, a complex IS is not only evaluated as positive or negative but also includes various positive and negative attributes, and users can simultaneously experience both attributes.

Second, enablers and inhibitors can have different antecedents. Focusing on only positive or negative antecedents, as is the case in research using the technology acceptance model, leads to an incomplete set of factors in IS research. Distinguishing between inhibitors and enablers helps identify their respective antecedents, which consequently influence IS usage intention. For example, enablers can be generated from the influence of highly suited applications for system design purposes or an individual's positive per-

ceptions of quality for IS, whereas inhibitors can be generated from the carelessness of not considering the system's various risk factors.

Third, the enablers and inhibitors affect the intention to use IS independently of each other. Enablers and inhibitors can have positive and negative effects, respectively, on usage intentions. Further, inhibitors can hinder the intentions despite the presence of enablers facilitating those same intentions, and a negative impact can exist with no correspondingly positive antipole. The reverse is also possible.

As aforementioned, the dual-factor theory argues that the enabler and inhibitor factors in IS can coexist independently and that individuals can simultaneously hold the perceptions of both inhibitors and enablers. Because the P–P paradox is about two contradictory factors existing simultaneously, the dual-factor theory is suitable for understanding the coexistence of positive and negative factors when using IoT services. Moreover, this theory can serve as a theoretical background for enablers and inhibitors to have different antecedents. Thus, this study uses the dual-factor theory to derive the personalization of IoT services as a key enabler for IoT use and information privacy concerns of IoT services as a key inhibitor through a literature review of existing research on the privacy paradox in IS. This study verifies whether these paradoxical factors affect the use intention of IoT and are influenced by different antecedent factors. The next subsection describes the antecedents.

Using the dual-factor theory [16,17], the conceptual framework in this study is established using paradoxical dual factors (enabler and inhibitor), with each factor having different antecedents, on the intention to use IoT. Figure 1 presents the conceptual framework of this study.

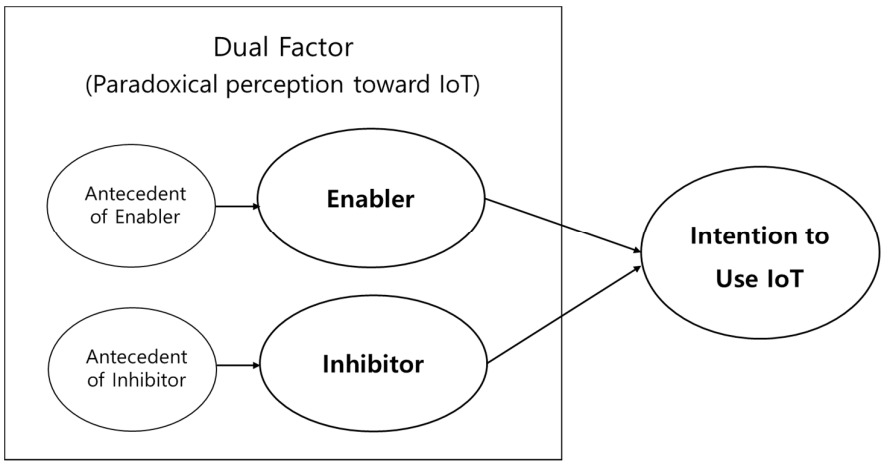

Figure 1. Conceptual framework.

2.3. Antecedents of the Dual Factor: Motivated Innovativeness and Previous Privacy-Invasion Experience

Personal innovativeness needs to be present for an evolved service, such as a personalized service using IoT technology, to be adopted [19]. Innovativeness is an individual's willingness to attempt a new idea, technology, or service [35]. Personal innovativeness is a specific individual trait that has long been studied in the domains of innovation diffusion and new technology adoption [12]. Individuals with high innovativeness have propensities such as active information seeking, more openness toward new things, and greater exposure to media [36]. Prior studies on the P–P paradox considered personal innovativeness as a focal antecedent related to personalization. For example, Xu et al. [12] and Zhao et al. [21] asserted that personal innovativeness positively influences the willingness to disclose personal information when using location-based personalized services. Vinodh and Mathew [37] explained that innovativeness, an expression of novelty seeking that motivates individuals, can affect the behavioral intention to use a new technology. However, personalization can influence the relationship between an individual's motivated innovativeness and intention to use online services [37]. Kim and Kim [18] asserted that personal

innovativeness positively affects the perceived benefits of personalized recommendations, such as the perceived usefulness and convenience of personalized services. Therefore, individuals with more motivated innovativeness are more interested in personalizing IoT services.

Regarding the adoption of high-technology products and services, previous studies often addressed innovativeness as a single dimension, whereas recent research suggested a multidimensional construct [38–40]. These studies classified multiple types of innovativeness by referring to the four-dimensional motivated consumer innovativeness proposed by Vandecasteele and Geuens [20]. Vandecasteele and Geuens [20] proposed a multidimensional motivated consumer innovativeness scale to better understand the effects of individuals' different motivated innovativeness as follows: (1) cognitive innovativeness refers to innovativeness motivated by mental stimulation and cognitive goals, including intellectual exploration and creativity; (2) functional innovativeness refers to innovativeness motivated by the functional performance of innovations that focuses on task goals and accomplishment improvement; (3) hedonic innovativeness refers to innovativeness motivated by affective stimulation and gratification; and (4) social innovativeness refers to innovativeness motivated by the self-assertive social need for differentiation. When addressing the differences among individuals in terms of both the level and type of innovativeness, the innovativeness scale needs to be more balanced. This study applies this four-dimensional motivated innovativeness to analyze the effects of different types of innovativeness on IoT service personalization.

In previous studies on the P–P paradox, privacy-invasion experiences were examined as a key antecedent of privacy concerns or perceived risks [6,10,41]. When people provide personal information to service providers, they expect that service provider companies will properly manage users' personal information given the responsibility from the implied or expressed contracts between users and these companies [42]. However, users consider their contract with service companies breached if their personal information is misused, such as when information is opened to or shared with other parties without their permission [12]. Such a negative experience can make individuals very careful about services that use personal information. Particularly, if an individual has a strong loss aversion, which weighs losses more heavily than gains, then they care to ensure that any experienced loss or regret is not repeated, thereby increasing concerns about privacy protection [22]. People with such a strong loss aversion generally have a status quo bias, making them reluctant to use new information and communication technology (ICT) services [22,43]. Thus, individuals who have been victims of the abuse of personal information can have stronger information privacy concerns [44], thus decreasing their intention to use IoT services. Previous privacy-invasion experiences include direct experiences wherein the information subject perceives that their information has been infringed on and indirect experiences wherein people are informed through media reports of people's information being misused or abused [44]. In other words, a previous privacy-invasion experience refers to the degree of the direct or indirect experience to which an individual has been exposed or that an individual has suffered because of damage to online privacy. Individuals who previously experienced invasions of direct or indirect privacy are less likely to participate in online personal profiling due to their privacy concerns [41].

Meanwhile, many studies demonstrated a positive relationship between past privacy-invasion experiences and privacy concerns; however, their analysis results were not always significant. For example, in a study on the privacy paradox in a location-based SNS, previous privacy invasions did not significantly affect privacy concerns. However, Garg and Kim [45] explained that users' attitudes toward IoT services depend on their past experiences and understating of technology, which makes examination of the influence of past experiences necessary. Therefore, through a literature review, this study identifies and investigates previous privacy-invasion experiences as a key antecedent factor that influences privacy concerns regarding IoT.

3. Research Model and Hypotheses

To investigate the P–P paradox phenomenon emerging in IoT, this study proposes a research model that utilizes the dual-factor theory as well as a literature review. As shown in the conceptual framework of this study in Figure 1, the research model includes a paradoxical dual factor (enabler and inhibitor), the dual factor's antecedents, and a dependent variable of intention to use IoT services. This model analyzes the impact of the dual factor—personalization and information privacy concerns related to IoT services—on the intention to use IoT. According to the dual-factor theory, the enabler and inhibitor factors have different antecedent factors [17]. Therefore, in this study, key antecedent variables, which affect each factor, were derived through a literature review of extant studies on personalization and privacy concerns related to IoT and Internet services, as noted in Section 2. This research posits that motivated innovativeness with four dimensions (cognitive, functional, hedonic, and social) is a key factor that influences the personalization of IoT services and that previous privacy-invasion experience is a key antecedent for the information privacy concerns related to IoT. Then, to examine the moderating effects on the P–P paradox, this study model utilizes the type of IoT service and the type of IoT user value as moderators. Figure 2 illustrates the proposed research model.

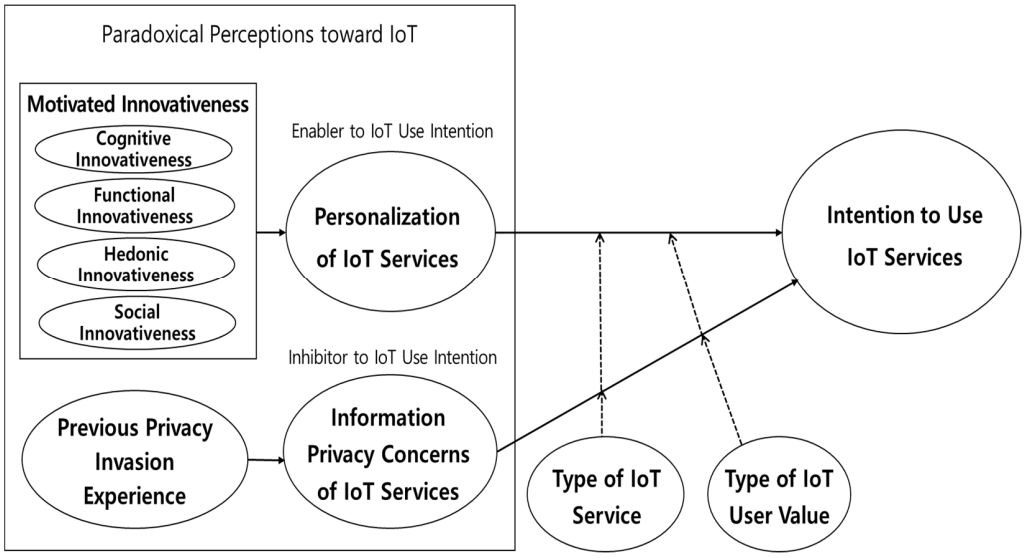

Figure 2. Research model.

In the following subsections, research hypotheses on the relationship between the dual factor and its antecedents, the relationship between the dual factor and dependent variable, and the moderating effects of this study are presented.

3.1. Personalization of IoT Services and Antecedent

Personalization is about the ability to provide content or services tailored to individuals through the use of personal information [12]. This use of personal information is central to the definition of personalization as understanding and meeting one's wants and needs [46]. The degree of perceived personalization varies by individuals [44]. Guo et al. [25] and Xu et al. [12] defined personalization as the extent to which the customized services provided by service providers are based on personal information, such as a user's interests, preferences, tastes, behavior, identity, time, and location.

Users can be encouraged to disclose their personal information in exchange for personalized services [33]. The personalization of services occurs when the services are optimized to an individual user's information [12]. A major competitive advantage strategy for enterprises is providing personalization through Internet-based businesses. Furthermore, service providers can utilize ICT to better communicate with users and offer superior personalized services by effectively collecting and analyzing personal information [4,47].

In today's highly competitive environments, firms need to use personal information to attempt to provide personalized services for customers to increase customer loyalty [41,48]. Therefore, personalization is central to increase the use of an IoT service. In this study, personalization of IoT services is identified as a key enabler with positive effects on use intention for IoT. Therefore, the following hypothesis is proposed.

Hypothesis 1 (H1). *Personalization positively affects the intention to use IoT services.*

Personal innovativeness is an essential factor to understand the propensity for ICT acceptance [19,49]. The perceived attraction toward new ICT services can vary depending on individuals' degrees of motivated innovativeness [49]. Kwon et al. [50] demonstrated that personal innovativeness can positively affect the perceived usefulness of context-aware services tailored to the personal context. Kim and Kim [18] claimed that personal innovativeness positively influences the perceived benefits of personalized recommendation services. Further, innovativeness can be positively related to the willingness to disclose personal information to obtain more personalized services [12]. Thus, individuals who are motivated with higher innovativeness are more positively aware of the personalization provided by IoT services. Innovativeness can be classified into four dimensions: cognitive, functional, hedonic, and social [20,38–40].

People with high cognitive innovativeness tend to prefer cognitively stimulating experiences, such as learning how to operate an innovative product and service in practice [51]. Individuals with cognitive innovativeness are likely to get involved with mentally demanding activities, such as deeply processing information or rational judgment [20,52]. Generally, new products/services based on advanced technologies such as IoT have a highly innovative nature. Therefore, cognitively motivated individuals may find that a new experience using such a product/service is mentally stimulating and will exert more effort to comprehend the product/service by following the central processing route, leading to an increase in the individual's comprehension of the new product/service [40]. Individuals who are motivated with higher cognitive innovativeness are expected to more positively perceive IoT service personalization because it provides cognitively stimulating experiences. Thus, the following hypothesis is developed.

Hypothesis 2 (H2). *Cognitive innovativeness is positively related to the personalization of IoT services.*

When individuals are motivated by functional innovativeness, they particularly emphasize the attributes of utilitarianism, such as the functional reliability, durability, and quality of products and services. Such individuals seek products and services that provide functional innovation [53,54]. New products/services, such as new ICT-based products/services related to IoT, that are designed to solve consumer problems that cannot be solved using existing products/services allow consumers to perform the tasks that they are unable to perform using existing technologies [55]. When people have high utilitarian motivation and functional needs, they are highly aware of these functional task accomplishments provided by the products/services [40,56]. Therefore, individuals motivated with higher functional innovativeness are expected to more positively perceive the personalization of IoT services because it provides them with optimized functions. Thus, the following hypothesis is proposed.

Hypothesis 3 (H3). *Functional innovativeness is positively related to the personalization of IoT services.*

Hedonic innovativeness is the tendency to use or purchase innovative products and services for enjoyment and affective satisfaction [20]. Hedonic motivation affects technology acceptance [57]. More hedonically innovative individuals enjoy products/services when they are more interesting and suit their tastes or provide a more sensuous service

that fits individuals' emotions. Such features encourage individuals to pay attention to and learn more about the products/services [40,58]. Hwang et al. [38] revealed that hedonically motivated innovativeness can positively influence consumers' perceived image of the evolved service, such as robotic technology-based services. Therefore, individuals motivated with higher hedonic innovativeness are expected to more positively perceive the personalization of IoT services because it provides the type of information and services that they might like considering their personal preferences and interests. Thus, the following hypothesis is proposed.

Hypothesis 4 (H4). *Hedonic innovativeness is positively related to the personalization of IoT services.*

Social innovativeness is related to social situations and seeks to improve self-expression in social status through the use of innovative products and services [59,60]. Some people develop their ideal identities by possessing new products or showing their use of advanced services [61]. For people with a strong social motivation, this possession and use of new products/services are socially acceptable ways to develop their unique images and impressions [62]. If the use of a product/service can be a source of social pride, individuals with strong social innovativeness are expected to become more interested in the product/service [59]. Therefore, individuals who are motivated with higher social innovativeness are expected to more positively perceive the personalization of IoT services because it is recognized as socially advanced. Thus, the following hypothesis is proposed.

Hypothesis 5 (H5). *Social innovativeness is positively related to the personalization of IoT services.*

3.2. Information Privacy Concerns of IoT Services and Antecedents

Privacy concerns can coexist because users are likely to seek personalized services [30]. A privacy concern is the concern about one's privacy being violated by external environmental factors and the possibility of loss of privacy as a result of the spontaneous or involuntary disclosure of personal information [63]. Privacy concerns might appear differently depending on individual characteristics—even under the same conditions [64]. Recent studies on privacy have not been concerned with privacy per se but have focused more on investigating information privacy concerns [26,30]. The general concept of information privacy is related to an individual's ability to maintain their territory by restricting others' access to their information and the claim to determine for themselves when, how, and to what extent personal information is communicated to others [65]. The information privacy concern represents an individual's subjective view of fairness about the domain of information privacy [44,65]. Information privacy concerns related to personal information include concerns over excessive collection, secondary uses as non-purpose uses, unauthorized access, and errors [44].

In the information age, people are aware of and are concerned that their privacy can be violated through monitoring and observation facilitated by evolving ICT [66]. Particularly, IoT is characterized by its inherent connectivity and cohesion, which increase the possibility that an individual's personal information is exposed, thereby leading to information privacy issues. When people are concerned about information privacy related to IoT, the belief that providing plenty of personal information increases the expected potential loss could eventually negatively affect the intention to use IoT services that utilize personal information. Individuals with strong privacy concerns might consider discontinuing their services and moving to other services [67], and their intentions to use IoT could decrease. Therefore, the following hypothesis is proposed.

Hypothesis 6 (H6). *Information privacy concerns negatively affect the intention to use IoT services.*

Personal experience drives individual behavior in activities that can be considered subjectively in relation to privacy [41]. Previous experience can be related to future expectations, and negative past experience might lead to pessimistic perspectives, such as causing bloated worries about possible recurrences [21]. Individuals with more negative privacy experiences can be less optimistic about online risks related to privacy than those with minimal or no privacy-invasion experiences [68]. Previous studies on location-based services revealed that previous privacy-invasion experiences can increase users' privacy risk perceptions and privacy concerns [12,69]. People are concerned that service providers collect and use personal information without their consent, and those who have experienced direct or indirect damage from the misuse of personal information could be more concerned about privacy [70]. Therefore, the following hypothesis is proposed.

Hypothesis 7 (H7). *Previous privacy-invasion experience is positively related to information privacy concerns over IoT services.*

3.3. Moderating Effects of Type of IoT Service and IoT User Value

In some cases, IoT services that have been used once are either continuously used or are not used at all. For example, Meyer et al. [24] reported that approximately one-third of activity tracking device (one of the smart healthcare services) users in the United States stopped using IoT services within six months. Data from Business Insider Intelligence [71] showed that some users who use smart speakers at home employ various voice assistant applications a few times, but not later. Garg [25] attempted to explain that the reasons for continuing to use or not use IoT can vary across different types of IoT services. Garg [25] performed a qualitative content analysis to understand IoT (non) use practices and decisions. The content analysis results suggested that people do not use IoT services when they do not feel in control, have various information privacy concerns over the service, and perceive that the service fails to understand their personal intent. In a study on the privacy paradox, Xu et al. [12] showed that the effect of personalization can vary by type of service depending on the personal information utilization system. Currently, many types of IoT services exist, such as smart homes—including artificial intelligence smart home speakers such as Echo—smart healthcare solutions, smart cars, and smart wearable communication devices, including smart glasses and smart watches, among others. Depending on these types of IoT services, the influence of the P–P dual factor on the use intention for IoT can vary. Thus, this study attempts to investigate the moderating effect of the type of IoT service and develops the following hypotheses.

Hypothesis 8 (H8). *The type of IoT service moderates the relationship between personalization and the intention to use IoT.*

Hypothesis 9 (H9). *The type of IoT service moderates the relationship between information privacy concerns and the intention to use IoT.*

Whereas various IoT services are developed competitively, the values that users truly want and experience must be provided if these services are to be settled in people's lives and if the service market is to grow further. Users' perceived value of using IoT can be a significant factor in the continuous use of IoT services [72]. In previous studies on the P–P paradox, the perceived value of services was found to significantly affect the intention to use ICT-based services [12,31]. However, the influence of the P–P paradox factors on the intention to use might vary depending on the value that a user deems important. The study by Awad and Krishnan [41] on the privacy paradox found that the impact of personalization can vary depending on the aspects that users value. A user's decision to further use or stop an IoT service could differ depending on the service's primary purpose and value [25]. For example, the primary purpose of a service might be safety during an emergency or to remotely control and manage objects; this value could moderate the association between the dual-factor (enabler and inhibitor) and the intention to use IoT.

Because value can be defined in various ways [73], this study primarily focuses on terms such as user or customer value, and "user value" refers to the evaluation of what users value about products or services [74]. Therefore, IoT user value means the user's perceived evaluation of IoT services.

IoT services have various types of user values. Park and Ryoo [75] classified IoT user values into the following 11 types, with this classification reflecting the prior literature review on the value perceived by these users: (1) Manageability: using IoT allows people to remotely monitor and manage a situation from the inside and outside as well as anytime and anywhere. (2) Automation: IoT automatically suggests or executes a customized service that is suitable for the individual without special effort. (3) Scalability: using IoT enables connection and expansion with new devices, technology, and services. (4) Safety: using IoT can proactively prevent and protect against accidents or external physical threats that might occur in specific spaces. (5) Economic efficiency: using IoT services comes with economic benefits in terms of cost, time, and effort. (6) Speed: IoT services can be used quickly, anytime, and anywhere. (7) Relativity: using IoT helps build consensus among users (e.g., family members), increases communication, and strengthens social relationships. (8) Familiarity: IoT provides human-friendly interfaces and services that make IoT-connected products feel familiar and comfortable. (9) Information: IoT provides the necessary information in an appropriate and efficient manner. (10) Entertainment: individuals have fun and are entertained when using IoT services. (11) Environmentality: by using IoT, the surrounding environment, including its temperature, humidity, and air condition, are more purified, thereby contributing to a healthier life. This study applies these IoT user value types proposed by Park and Ryoo [75]. When using a certain IoT service, IoT users will perceive a value as the most important. For example, a smart home service can provide various types of user value, including manageability, automation, safety, and speed. Among these values, a user could consider one value as most important, which can make users continue to use IoT. Depending on the type of IoT user value that a user perceives as important, in some cases, only personalization—optimized for an individual through the use of personal information—significantly affects the use intention for IoT. In some cases, only the impact of privacy concerns can be significant. Additionally, both P–P factors might or might not be important for increasing use intention. Thus, this study attempts to investigate the moderating effect of the type of IoT user value and develops the following hypotheses.

Hypothesis 10 (H10). *The type of IoT user value moderates the relationship between personalization and the intention to use IoT.*

Hypothesis 11 (H11). *The type of IoT user value moderates the relationship between information privacy concerns and the intention to use IoT.*

4. Research Method

4.1. Data Collection and Sample

The data used in this study were collected through a web-based survey. The survey participants were recruited through a professional survey agency that has been conducting various survey projects since its founding in 1978. This agency is a large professional survey organization in South Korea. Only individuals with experience in using IoT services were surveyed. A web survey was conducted with IoT users aged 15 years or older. On the first page of the web survey questionnaire, the purpose and subject of this study were introduced, and confidentiality was guaranteed. First, while explaining the purpose and subject of this study, the definition of IoT concept and IoT services were presented in detail, so that only those with an understanding of these IoT services could be invited to take the survey. Next, survey participants were asked to answer whether they had experience in using IoT services. Only those who answered affirmatively were allowed to answer the following questions, while the others were filtered out. Meanwhile, many types of IoT

services exist: smart homes, smart healthcare, smart cars, smart wearable communication, smart grids, smart buildings, smart cities, smart farms, and smart factories, among others. Respondents were asked to select the IoT service that they use most frequently and choose the user value that they perceive as most important when using IoT services from among the 11 value types proposed by Park and Ryoo [75].

The survey was conducted from 20 June to 2 July 2019. Data were collected using the stratified random sampling method that takes a random sample within each stratum based on gender and age groups; that is, data were collected in almost the same proportion by gender and age groups because this research seeks to evenly understand the perception and experience of IoT according to gender and age groups. In this study, stratified random sampled data were collected. By the time this survey was concluded, 311 questionnaires were collected. After removing incomplete responses, the final sample comprised 306 responses. Table 2 provides a profile of the sample.

Table 2. Sample characteristics.

Category		Frequency	Percent
Gender	Men	153	50.0
	Women	153	50.0
	18–29	81	26.5
	30–39	83	27.1
	40–49	72	23.5
	Over 50	70	22.9
Education	High school or below	35	11.4
	Undergraduate	21	6.9
	University	212	69.3
	Graduate school	38	12.4
Job	Office worker	140	45.8
	Professional	57	18.6
	Student	34	11.1
	Housewife	33	10.8
	Inoccupation	16	5.2
	Self-employed	15	4.9
	Civil service	11	3.6
Average Monthly Household Income	Less than USD 850	11	3.6
	USD 850–1700	18	5.9
	USD 1700–2550	63	20.6
	USD 2550–3400	54	17.6
	USD 3400–4250	52	17.0
	More than USD 4250	108	35.3
Period of IoT usage	Less than 6 months	124	40.5
	6 months–1 year	82	26.8
	1 year–2 years	53	17.3
	2 years–3 years	28	9.2
	Longer than 3 years	19	6.2
IoT Service Type	Smart home	199	65.0
	Smart healthcare	46	15.0
	Smart wearable communication	37	12.1
	Smart car	14	4.6
	Smart building	3	1.0
	Smart farm	3	1.0
	Smart factory	3	1.0
	Smart grid	1	0.3

Table 2. *Cont.*

Category		Frequency	Percent
IoT User Value Type	Manageability	83	27.1
	Automation	96	31.4
	Scalability	17	5.6
	Safety	29	9.5
	Economic efficiency	17	5.6
	Speed	21	6.9
	Relativity	4	1.3
	Familiarity	2	0.7
	Information	30	9.8
	Entertainment	4	1.3
	Environmentality	3	1.0

4.2. Measurements

To measure these research variables, existing validated scales were adapted for the context of this study. Each variable included multiple items measured on seven-point Likert scales. To ensure the face validity of the measurement items, a pilot test was conducted using 10 undergraduate students and 5 graduate students who understood what IoT services are. These students were not part of the final sample. This study tested face validity as an assessment method for judging which items are appropriate to the targeted construct [76]. After testing face validity in the pilot test, minor wording changes were made to clarify the items' meanings. Table 3 provides the operationalized definitions of these research variables, and Table A1 in Appendix A presents specific measurement items.

Table 3. Operationalized definitions of variables.

Variable	Operationalized Definition	References
Cognitive Innovativeness	Degree of innovativeness motivated by mental stimulation and cognitive goals	[20,60]
Functional Innovativeness	Degree of innovativeness motivated by the functional performance of innovations	
Hedonic Innovativeness	Degree of innovativeness motivated by affective stimulation and gratification	
Social Innovativeness	Degree of innovativeness motivated by the self-assertive social need for differentiation	
Previous Privacy Invasion Experience	Degree of direct or indirect experience that an individual has been exposed to or suffered from in terms of the damage of privacy online	[12,70]
Personalization of IoT Services	Degree of perception that IoT services are tailored to individual preferences and situations based on personal information	[12,30,77]
Information Privacy Concerns of IoT Services	Degree of concerns over the possibility that personal information collected by IoT providers may lead to privacy violations from intentional or unintentional misuse and abuse	[44,65]
Intention to Use IoT Services	Degree of willingness to use IoT services	[78]

5. Data Analysis and Results

The proposed model was tested using structural equation modeling supported by partial least squares (PLS), SmartPLS version 3.3.3, which has been widely used in prior research and supports simultaneous testing of the measurement and structural models [79].

5.1. Measurement Validation

To validate the measurement instrument, confirmatory factor analysis (CFA) using PLS was conducted. The convergent validity and reliability of the measurement model were evaluated by examining item-construct loading, composite reliability (CR), Cronbach's alpha, and average variance extracted (AVE) [80]. Table 4 presents the results of the CFA. All standardized factor loadings were greater than the threshold of 0.6 [81], CR and Cronbach's alpha for all of the constructs exceeded 0.7, and the AVE for each construct was greater than 0.5, all of which were the recommended threshold values [80,82]. As all conditions were met, the convergent validity and reliability of the measurements were established.

Table 4. Results of testing convergent validity and reliability.

Construct	Item	Factor Loading	AVE	Composite Reliability	Cronbach's Alpha
Cognitive Innovativeness (COI)	COI1	0.884	0.808	0.944	0.921
	COI2	0.909			
	COI3	0.897			
	COI4	0.905			
Functional Innovativeness (FUI)	FUI1	0.838	0.713	0.925	0.899
	FUI2	0.881			
	FUI3	0.843			
	FUI4	0.805			
	FUI5	0.853			
Hedonic Innovativeness (HEI)	HEI1	0.887	0.811	0.945	0.922
	HEI2	0.902			
	HEI3	0.910			
	HEI4	0.902			
Social Innovativeness (SOI)	SOI1	0.833	0.772	0.944	0.926
	SOI2	0.888			
	SOI3	0.909			
	SOI4	0.905			
	SOI5	0.856			
Previous Privacy Invasion Experience (PPI)	PPI1	0.675	0.634	0.873	0.808
	PPI2	0.817			
	PPI3	0.871			
	PPI4	0.809			
Personalization of IoT Services (PER)	PER1	0.877	0.794	0.964	0.957
	PER2	0.896			
	PER3	0.910			
	PER4	0.895			
	PER5	0.892			
	PER6	0.886			
	PER7	0.881			
Information Privacy Concerns of IoT Services (IPC)	IPC1	0.778	0.816	0.969	0.962
	IPC2	0.910			
	IPC3	0.932			
	IPC4	0.929			
	IPC5	0.928			
	IPC6	0.931			
	IPC7	0.907			
Intention to Use IoT Services (INT)	INT1	0.921	0.836	0.953	0.935
	INT2	0.922			
	INT3	0.918			
	INT4	0.896			

The discriminant validity of the measurement model was examined by comparing the square root of AVE for each construct with the inter-construct correlations [82]. As Table 5 shows, the square root of AVE for each construct was larger than all of the related inter-construct correlations, thus establishing the discriminant validity of all of the scales. Additionally, the variance inflation factor (VIF) scores were assessed to check for multicollinearity among the constructs. The resultant VIF scores ranged from 1.056 to 2.555, which were lower than the recommended threshold value of 10 [83]. Thus, there was no multicollinearity problem in this study. The extent of common method bias was tested with Harman's one-factor test [84], which assesses whether a single factor accounts for greater than 50% of the variance. The results showed that no factor significantly dominated the explanation of variance (with the most influential factor accounting for 17.214% of the variance); thus, there is no common method bias problem in this study.

In sum, the results of testing the instrument validity indicate the adequacy of the measurement model used in this study.

Table 5. Correlation matrix and square roots of AVE [1].

	PER	PPI	IPC	SOI	FUI	HEI	COI
PER	**0.891**						
PPI	0.194	**0.796**					
IPC	0.231	0.449	**0.904**				
SOI	0.456	0.167	0.086	**0.879**			
FUI	0.578	0.233	0.179	0.578	**0.844**		
HEI	0.589	0.219	0.149	0.677	0.678	**0.900**	
COI	0.576	0.089	0.103	0.671	0.671	0.684	**0.899**

[1] The leading diagonal in bold shows the square root of each construct's AVE.

5.2. Hypotheses Testing

The structural model was examined using PLS. To test the hypotheses, the path coefficients and statistical significance were analyzed. Figure 3 presents the results of the structural model analysis. As hypothesized, the personalization of IoT services showed a significant positive effect on the use intention for IoT, thereby supporting Hypothesis 1. However, unlike the expected impact, the information privacy concerns of IoT services did not significantly affect the use intention; thus, Hypothesis 6 is not supported. Cognitive, functional, and hedonic innovativeness had significant positive effects on the personalization of IoT, thereby supporting Hypothesis 2, Hypothesis 3, and Hypothesis 4. Meanwhile, the path between social innovativeness and personalization was not significant; thus, Hypothesis 5 was not supported. Previous privacy-invasion experience had a significant positive effect on the information privacy concerns of IoT, thereby supporting Hypothesis 7.

To verify the moderating effects of IoT service type, this study compared the relationships between the dual factor and the intention to use among the IoT service types, following the two-step procedure employed by Keil et al. [85]. First, for each of the groups, the use intention was regressed on the dual factor. Table 6 presents the first step regression results. Second, the corresponding path coefficients (e.g., personalization → intention) in the groups' regression models were statistically compared using the *t*-test from Keil et al. [85]. This comparison was conducted for only the paths that were significant in both groups. Regarding the results in the second step, a significant *t*-value from the *t*-test between the corresponding path coefficients indicates that the difference for that particular path between groups is statistically significant [86,87]. A comparative analysis among IoT service types was conducted for a total of 4 IoT services only with 10 or more samples in the group [88]—that is, smart home, smart healthcare, smart car, and smart wearable communication. In Table 6, the analysis results of the IoT service type groups showed that the significant paths differed among IoT service types. In terms of the personalization–intention relationship, statistically significant differences existed in the path coefficients among IoT service types, as shown in Table 7. The influence of personalization was the

highest for smart home and smart car and was lowest for smart healthcare. Meanwhile, the impact of information privacy concerns on use intention was significant only for smart healthcare and smart wearable communication. Particularly, its influence was positive for smart healthcare. The results of this analysis showed that the effects of P–P on use intention differed depending on IoT service type. Thus, Hypothesis 8 and Hypothesis 9 were supported.

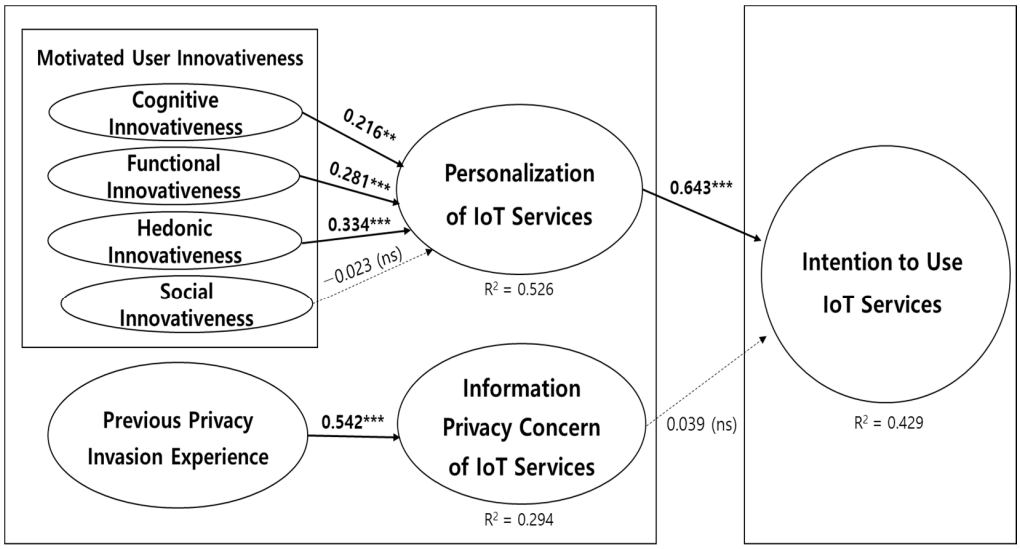

Figure 3. Results from testing of the structural model.

Table 6. Results obtained from testing of the relationship between the dual factor and intention among IoT service types.

Path	Path Coefficient			
	Smart Home	**Smart Healthcare**	**Smart Car**	**Smart Wearable Communication**
Personalization → Intention to Use IoT	0.672 ***	0.539 ***	0.672 **	0.639 ***
Information Privacy Concerns → Intention to Use IoT	0.021 (ns)	0.251 *	0.236 (ns)	−0.244 *

*: $p < 0.05$; **: $p < 0.01$; ***: $p < 0.001$; ns: not significant (two-tailed).

Table 7. Results of comparative testing of path coefficients among IoT service types.

Path	Path Coefficient (Standard Error)	Between Groups	*t*-Value by *t*-Test [1]
Personalization → Intention to Use IoT	HO: 0.672 (0.057) SC: 0.672 (0.274) WC: 0.639 (0.167) HC: 0.539 (0.096)	HO vs. SC HO vs. WC HO vs. HC SC vs. WC SC vs. HC WC vs. HC	0.000 (ns) 2.197 * 12.321 *** 0.523 (ns) 2.814 ** 3.422 ***
Information Privacy Concerns → Intention to Use IoT	HC: 0.251 (0.098) WC: −0.244 (0.146)	HC vs. WC	18.420 ***

HO = Smart Home; SC = Smart Car; WC = Smart Wearable Communication; HC = Smart Healthcare. *: $p < 0.05$; **: $p < 0.01$; ***: $p < 0.001$; ns: not significant (two-tailed). [1] *t*-test is conducted using the following formula of Keil et al. [49]. *t*-value = (PC1 − PC2)/[Spooled × $\sqrt{}$(1/N1 + 1/N2)]; where Spooled = pooled estimator for the variance; Spooled = $\sqrt{}${[(N1 − 1)/(N1 + N2 − 2)] × $SE1^2$ + [(N2 − 1)/(N1 + N2 − 2)] × $SE2^2$}; Ni = sample size of dataset for group I; SEi = standard error of path in structural model of group I; PCi = path coefficient in structural model of group i.

Finally, to verify the moderating effect of the type of IoT user value, a comparative analysis among user value groups was conducted through the same procedure for Hypothesis 8–Hypothesis 9 for a total of 7 groups with 10 or more samples in the group [88]—specifically, these included manageability, automation, scalability, safety, economic efficiency, speed, and information. The regression results of the sub-groups in Table 8 show that the significant paths differed among IoT user value types. Regarding the path from personalization to use intention, statistically significant differences existed in the path coefficients among IoT user value types, as presented in Table 9. The effect of personalization was the highest for economic efficiency and the second highest was for speed and information, followed by manageability, automation, and safety. The impact of the information privacy concerns on use intention was significant only for manageability; for other user value types, although the path coefficients were not significant, the direction of the influence of privacy concerns on use intention was positive for some value types and negative for others. As a result of this analysis, the effects of P–P on use intention differed depending on the type of IoT user value that IoT users considered important. Thus, Hypothesis 10 and Hypothesis 11 were supported.

Table 8. Results obtained from testing of the relationship between the dual factor and intention among IoT user value types.

Path	Path Coefficient						
	Manageability	**Automation**	**Scalability**	**Safety**	**Economic Efficiency**	**Speed**	**Information**
Personalization → Intention to Use IoT	0.624 ***	0.594 ***	0.251(ns)	0.514 **	0.928 ***	0.778 ***	0.767 ***
Information Privacy Concerns → Intention to Use IoT	0.186 *	0.069 (ns)	0.199 (ns)	−0.072 (ns)	−0.089 (ns)	0.115 (ns)	−0.062 (ns)

*: $p < 0.05$; **: $p < 0.01$; ***: $p < 0.001$; ns: not significant (two-tailed).

Table 9. Results of comparative testing of path coefficients among IoT user value types.

Path	Path Coefficient (Standard Error)	Between Groups	*t*-Value by *t*-Test
Personalization → Intention to Use IoT	EC: 0.928 (0.136) SP: 0.778 (0.246) IN: 0.767 (0.118) MA: 0.624 (0.083) AU: 0.594 (0.092) SF: 0.514 (0.149)	EC vs. SP	2.248 *
		EC vs. IN	4.253 ***
		EC vs. MA	12.184 ***
		EC vs. AU	12.751 ***
		EC vs. SF	9.385 ***
		SP vs. IN	0.213 (ns)
		SP vs. MA	4.779 ***
		SP vs. AU	5.771 ***
		SP vs. SF	4.716 ***
		IN vs. MA	7.186 ***
		IN vs. AU	8.380 ***
		IN vs. SF	7.243 ***
		MA vs. AU	2.276 *
		MA vs. SF	4.910 ***
		AU vs. SF	3.507 ***

EC = Economic efficiency; SP = Speed; IN = Information; MA = Manageability; AU = Automation; SF = Safety. *: $p < 0.05$; ***: $p < 0.001$; ns: not significant (two-tailed).

Additionally, this study tested the difference in the mean value of the research variables by demographic group factors (control variables), including gender, age, occupation, income, and education level. The ANOVA testing results show the differences among demographic groups. Among gender, significant differences existed for cognitive, hedonic, and social innovativeness, and intention to use IoT. Men showed higher degrees of difference than women. In age groups, the degree of perceived personalization showed a significant difference—it was the highest among young people aged between 18 and 29. In the occupation groups, significant differences were found in personalization, cognitive,

hedonic, and social innovativeness, and use intention for IoT, all of which were the highest in the student group. In the education level groups, significant differences existed among personalization and information privacy concerns, with information privacy concerns being the highest in the graduate school group, and personalization was the highest among undergraduate students. The income level groups showed no significant differences.

6. Discussion and Conclusions

6.1. Findings and Theoretical Contributions

Based on the dual-factor theory, this study empirically investigated the causes of people's usage, and other consequent phenomena, in relation to IoT services. Many previous studies examined the effects of perceived usefulness and ease of use on the attitude toward using new ICT services as well as the intent of use under the technology acceptance model framework. However, in this study, a different approach was employed to explain why individuals have a behavioral intention to use IoT based on the dual-factor theory and the P–P paradox perspective.

Particularly, the four-dimensional motivated innovativeness was expected to influence personalization in IoT services. The results of this study demonstrate the following. First, cognitive innovativeness, which satisfies individuals' intellectual needs, can help with the fact that more attention is paid to personalized IoT services. Second, functional innovativeness, which is motivated by focusing on the performance of products' and services' utilitarian functions, increases the perceived personalization of IoT. Third, the hedonic innovativeness of individuals, which is related to affective stimulation, such as feelings of enjoyment and excitement when using new ICT products or services, can be an important factor in enhancing the perceived personalization of IoT. Specifically, hedonistic innovativeness had the greatest influence on personalization (the path coefficient for personalization was the largest among the motivating innovativeness factors). Thus, it can be interpreted that the use of IoT services can be most effectively facilitated when users are motivated to enjoy personalized IoT services. However, social innovativeness did not significantly affect the personalization of IoT. This result implies that individuals' social innovativeness, which is motivated by social impressions that differentiate one from others, is not directly associated with obtaining personalized IoT services. One possible explanation for this result is that the use of personalized IoT services has not yet been linked to social respect or the expression of an intentional impression regarding others, as argued by Esfahani and Reynolds [40]. Esfahani and Reynolds [40] studied consumer innovativeness regarding the adoption of very new products and argued that social innovativeness can influence different directions, unlike the other three aspects of innovativeness. They claimed that if a product/service is still too new and only a few early adopters exist, and it is unavailable for use for ordinary people, consumers could be less interested in the product/service in the near future because it is less helpful to them in terms of expressing themselves socially. Therefore, consumers' social-motivated innovativeness can negatively affect their attitudes toward products/services [40]. In the results of this study, although social innovativeness was not significant, it showed a negative path coefficient value. Therefore, it can be interpreted as being similar to the argument in the previous study [40]. Some existing research (e.g., [89]) has explained that innovativeness directly influences the intention to use; however, this study showed that the strengths of the personalization of IoT services is highly perceived when individuals' multifaceted innovativeness is high. Consequently, the willingness to continue using IoT services can increase. To further verify the role that personalization plays as a mediator, an additional analysis was conducted in this study. The analysis results showed that the effects of cognitive and functional innovativeness on use intention were fully mediated and that of hedonic innovativeness on use intention was partially mediated by personalization.

This study found that the perceived personalization performance of IoT services can enhance individuals' intention to use IoT. Garg [25] asserted that users are more likely to continue using IoT devices that do not require extra work and that fit easily

into their personal daily life routines. The result of this study is consistent with prior exploratory studies in that the main reason that users continue to use IoT can be the merit of personalized services tailored to their personal lives [25,45]. However, this study also showed that the degree of influence of personalization on use intention can be moderated by IoT service type and user value type. In the cases where the user uses certain IoT services (smart healthcare and smart wearable communication) and the value of manageability is highly perceived, the effects of P–P were found to coexist simultaneously.

Meanwhile, the results showed that information privacy concerns may not reduce the intention to use. This result can be interpreted as suggesting that most current users who have already attempted new IoT services do not have strong enough privacy concerns to stop using IoT. However, this study revealed that the influence of information privacy concerns on use intention can be moderated by IoT service type and user value type. For example, privacy concerns can be an inhibitor factor that negatively affects users' future use intention when using smart wearable communication devices. Additionally, this study demonstrated that people can be seriously concerned about their information privacy in relation to IoT when they have previous privacy-invasion experiences. Individuals might be highly aware of information privacy concerns given that they have experienced invasions of their privacy. Even if people perceive the advantages of personalized IoT services to be higher than the disadvantages of possible privacy leakage, when they have experienced personal information and privacy leakages several times, the negative perceptions from bad experiences can be accumulated and the concerns about privacy can be amplified; this might cause privacy concerns to outweigh the benefits of personalization. Therefore, IoT services' privacy protection is more important, especially for those who fear the risk of invasions of privacy when using IoT services because of their past negative experiences.

This study attempted to answer the following research agendas: (1) Although the P–P paradox could occur related to IoT, what are the main factors influencing IoT use intention? (2) Does the P–P phenomenon appear differently depending on the types of IoT services and user values? By solving these research agendas, this study contributes to gaining a better understanding of the factors influencing an increase in the intention to use IoT services. Existing research on IoT has primarily been conducted for a particular service rather than comparing the differences across several IoT services. The main factor for continuously using or not using IoT services could vary depending on the type of IoT service with different user values. Therefore, it is necessary to compare the differences according to service type and value type. To the best of the author's knowledge, this study is the first study to empirically investigate the moderating effects of IoT service type and user value type. Thus, this study can contribute to determining the aspects that should receive more attention in certain services with a specific value for encouraging the use of IoT services. In this study, the effects of the paradox variables on the behavioral intention to use IoT are verified through a comprehensive theoretical framework using the dual-factor theory, an approach that could serve as a useful theoretical foundation for future research on the privacy paradox phenomenon in the IoT context.

6.2. Managerial and Practical Implications

The results of this study yield managerial and practical implications for IoT service providers.

First, IoT service providers should focus on three types of innovativeness (cognitive, functional, and hedonic) and develop personalized IoT services that can stimulate such innovativeness. For example, users' hedonic innovativeness can drive the adoption of innovative IoT services that allow users to enjoy the novelty of personalized IoT services and spend their daily lives cheerfully. Hedonic innovative users could be more attracted through fun and experiential marketing. Additionally, IoT service providers can attempt activities such as promotions through social media that send the message that people with respected social status are better at utilizing personalized IoT services. Such messages make it possible to induce individuals with high social innovativeness to be more interested in

and use IoT services. Low et al. [90] asserted that companies have recently been investing in capabilities such as content and social influences that are optimized with smart digital marketing models and have been creating immersive digital multimedia experiences that motivate consumers to connect with their product and service. Additionally, companies are now investing in personalization as part of their digital strategies, making it easier for customers to obtain the information they want and to customize their needs in a smart and efficient way, thereby building a more loyal customer base to increase their sustainability as businesses [90]. Therefore, IoT service providers need to deliver and promote personalized service content that users can become immersed in and enjoy, and further strengthen digital marketing by leveraging social influence.

Second, the results of the analysis of a paradoxical attitude toward IoT reveal that the enabler (i.e., personalization) rather than the inhibitor (i.e., information privacy concerns) related to IoT usage has a stronger impact on the intention to use IoT services. Particularly, the effect of encouraging more people to use IoT can be stronger when users are well aware of the benefits of personalized IoT services. Hence, IoT service providers should invest more in implementing and publicizing personalized IoT services. However, issues related to protecting privacy should not be underestimated because the results of this study show that privacy concerns over IoT environments may increase because of previous privacy-invasion experience. Therefore, IoT service providers should be careful to not repeatedly cause personal information leakages and privacy invasions, which has happened in the past.

Third, designing and providing IoT services with reference to the differences in the P–P paradox among the types of IoT services and user values is necessary. The results of this study indicate that people who use smart home and smart car services place greater importance on the aspect of personalization of IoT rather than on privacy concerns. In particular, the effects of P–P on the use intention work independently in smart healthcare and smart wearable communication services. A comparison of the values of the path coefficients for these services showed that personalization has a larger coefficient value than information privacy concerns. However, although IoT services are still being used for the benefits of personalization, the consequence can be reversed if a situation occurs wherein the privacy invasion issue becomes more significant. For example, in this study, users of smart wearable communication services responded that their intention to use IoT might be lowered because of privacy concerns; therefore, in the case of IoT services that are provided by attaching devices to the individual body, such as smart watches or smart glasses, greater effort should be made to protect personal information and privacy. Additionally, IoT service providers should be aware that personalization needs to be more strongly emphasized depending on the value type perceived by IoT users as important. For example, if people appreciate the value of economic efficiency when using IoT, the possibility of continuing to use the service can be very high because of the advantage of personalization provided by IoT services. Moreover, users who want to use IoT for the value of manageability, such as enabling them to monitor and manage a situation remotely anytime and anywhere, will still use IoT even if they have some knowledge of the disadvantages related to privacy concern issues that might arise because of IoT. Furthermore, the results of the additional analysis indicate that the degrees of innovativeness, perceived personalization, and privacy concern might differ among demographic characteristics, such as gender, age, occupation, and education level. For example, in this study, the youngest age group of 18–29 had the highest positive perception about personalization of IoT services; therefore, it will be possible to provide more opportunities for young individuals to expand the experience of using personalized IoT services and to encourage them to spread information about the benefits of IoT services through word of mouth. Additionally, as people educated to a graduate-school level or higher were most concerned about information privacy, IoT service providers can consider presenting the contents about how to safely use IoT services through experts to give these highly educated people more confidence in using IoT services. Thus, the findings of this study indicate that firms in the IoT industry need to provide suitable services for target groups.

Based on what this study found, some recommendations for IoT service providers are presented as follows.

- First, check the main purpose and motive for using the IoT service you provide. Through this, closely understand what motivates your customers and what values they want to gain by using your IoT service; based on that, establish the service development and promotion strategy.
- Set the appeal points of your service according to the characteristics (age, education, gender, job, etc.) of your main target users. Will you appeal more to the latest personalization technology and advanced services? Or will you emphasize that your service is a secure IoT service with excellent information security?
- Figure out how users evaluate your services in terms of benefits through personalization and in terms of costs through privacy concerns. Particularly, if users assess both aspects to be significant, exercise caution so that the negative losses do not overwhelm the benefits.
- If an incident related to leakage of personal information or invasion of privacy occurs, notify the user immediately and clearly provide your solutions for solving the problems and take measures to prevent this from happening in the future; in this way, users can see your hard work and tolerate your service. Otherwise, your customers may leave you because of such negative experiences. Particularly, wearable IoT device providers should be more careful.

6.3. Conclusions, Limitations and Future Research

In conclusion, this study considered P–P factors based on the dual-factor theory, attempted to identify the antecedents of P–P factors, and verified the influence of P–P factors on the intention to use IoT. Further, it investigated the moderating effects by the type of IoT service and user value concerning the relationship between P–P factors and usage behavior. The outcome of this study can provide strategic insights for IoT researchers and IoT service providers to manage new challenges related to IoT.

However, this study has certain limitations.

First, four types of user innovativeness that affect perceived personalization related to IoT based on the literature were examined. However, other characteristics, such as involvement and ICT literacy, can also be investigated. In future studies, a review of additional variables might increase the explanatory power of this research model.

Second, this study employed a survey methodology because the research variables were related to individuals' cognitive and socio-psychological factors; thus, a survey was a suitable method for satisfying the research objectives. However, an experiment could be applied in future research as a complementary methodology to control exogenous variables and manipulate independent variables. An experimental design that could be used in a future study is the investigation of how some potential variables (e.g., the content of the personalized service) affect the behavioral intention to use IoT.

Third, the data used in this study were collected from one country (South Korea). The results might differ if data from other countries were used. For example, the degree of information privacy concerns may vary depending on the country, as there are differences in legal regulations for privacy protection in IoT in countries. Additionally, due to the extent of proliferation of IoT in countries, the influence of motivated innovativeness and perceived personalization in IoT could differ. Therefore, in future research, analyzing how cultural factors influence the hypotheses in this study would be interesting, and a comparative analysis by country can be conducted.

Fourth, among the IoT service type and user value type groups, there was a group with a small sample size in this study. In future research, it will be necessary to collect and analyze more sample sizes for each group. Particularly, in future research, more data on smart buildings and smart cities can be collected to conduct comparative studies on more diverse IoT services.

Fifth, in this study, the P–P paradox phenomenon was investigated from the perspective of IoT service users. However, future research will be able to explore ways to provide more efficient and secure IoT services from the point of view of IoT service developers and providers. For example, Cirillo et al. [91] proposed a method that can be shared and reused by smart city service developers through building applications composed of atomic service modules in smart city IoT services development, thus allowing expertise and know-how to be used cooperatively. Low et al. [90] proposed a digital marketing technology acceptance model that includes smartness indicators to enable the property development sectors to better facilitate the adoption of digital technologies. Therefore, in future studies, the possibility of IoT service developers and providers investigating key performance indicators they can build and components they can use to implement IoT services, while enhancing personalization and privacy protection, can be considered.

Funding: This research was funded by a 2018–2019 research grant from Sangmyung University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data are not publicly available due to participants' privacy.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A

Table A1. Measurement of variables.

Variable		Items	References
Cognitive Innovativeness	COI1	I largely buy innovative products (services) that satisfy my analytical mind.	[20]
	COI2	I tend to make purchases instantly when I find innovative products that need a lot of thinking and are intellectually challenging.	
	COI3	I mainly buy a new product that makes me think logically.	
	COI4	I am an intellectual thinker who buys a new product because it is likely to set and stimulate my brain to work.	
Functional Innovativeness	FUI1	If a new time-saving product (service) is launched, I am going to buy (use) it right away.	
	FUI2	If a new product affords me more comfort than my current product, I would not hesitate to buy (use) it.	
	FUI3	If a new product is more functional, I tend to buy (use) it.	
	FUI4	If I find a new product of a more convenient size, I am very inclined to buy (use) it.	
	FUI5	If a new product makes my work easier, I want to buy (use) it as much as possible.	
Hedonic Innovativeness	HEI1	Using a novel product (service) gives me a sense of enjoyment.	
	HEI2	Getting a new product gives me a good feeling.	
	HEI3	Acquiring a new product makes me happier.	
	HEI4	Discovering novelties makes me playful and cheerful.	
Social Innovativeness	SOI1	I like to use innovative products (services) that impress others.	
	SOI2	I like to use a new product that distinguishes me from others who do not own it.	
	SOI3	I prefer to try new products with which I can present myself to others.	
	SOI4	I like to outdo others by buying new products that my friends do not have.	
	SOI5	I deliberately buy novelties that are visible to others and that command respect or recognition from others.	

Table A1. *Cont.*

Variable		Items	References
Previous Privacy Invasion Experience	PPI1	I have suffered direct or indirect damage from improper privacy breaches.	[12,70]
	PPI2	I have frequently heard or read news reports and articles about the abuse and damage of personal information collected online.	
	PPI3	I experienced leakage of my personal information.	
	PPI4	I experienced a company using my personal information without my permission.	
Personalization of IoT Services	PER1	IoT services can provide me with personalized services tailored to my context.	[12,77]
	PER2	IoT services can provide me with more relevant information that meets my preferences and personal interests.	
	PER3	IoT services can provide me with the type of information and services that I might like and need.	
	PER4	IoT service providers can understand my personal consumption patterns and provide services tailored to me.	
	PER5	IoT services can provide me with what I want by collecting information about me.	
	PER6	IoT services can provide me with services that understand and meet my personal needs.	
	PER7	IoT services can provide me with individual services tailored to my lifestyle.	
Information Privacy Concerns of IoT Services	IPC1	I am concerned that using IoT services would cause me to lose control over the privacy of my information.	[30,70]
	IPC2	I am afraid that my personal information provided for use by IoT services could be abused.	
	IPC3	I am concerned that my personal information provided for using IoT services will be used for purposes other than the original.	
	IPC4	When using IoT services, I am worried that my personal information will be shared with other companies without any notice to me.	
	IPC5	I am afraid that my personal information will be leaked to unauthorized third parties without my consent.	
	IPC6	I am concerned that my personal information to IoT services may be used in an unexpected way.	
	IPC7	When using IoT services, collecting too much personal information about me is a concern.	
Intention to Use IoT Services	INT1	I am willing to use IoT services.	[78]
	INT2	I will use IoT services in the future.	
	INT3	I plan to use IoT services.	
	INT4	I will use IoT service without stopping it in the future.	

References

1. Statista. Internet of Things—Number of Connected Devices Worldwide 2015–2025. 2016. Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide (accessed on 11 September 2021).
2. Statista. Internet of Things (IoT) Total Annual Revenue Worldwide from 2019 to 2030. 2021. Available online: https://www.statista.com/statistics/1194709/iot-revenue-worldwide (accessed on 11 September 2021).
3. Pal, D.; Arpnikanondt, C.; Razzaque, M.A. Personal Information Disclosure via Voice Assistants: The Personalization-Privacy Paradox. *SN Comput. Sci.* **2020**, *1*, 1–17. [CrossRef]
4. Kim, D.; Park, K.; Park, Y.; Ahn, J.H. Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Comput. Hum. Behav.* **2019**, *92*, 273–281. [CrossRef]

5. Psychoula, I.; Singh, D.; Chen, L.; Chen, F.; Holzinger, A.; Ning, H. Users' Privacy Concerns in IoT Based Applications. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 8–12 October 2018; pp. 1887–1894.
6. Menard, P.; Bott, G.J. Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Comput. Secur.* **2020**, *95*, 101856. [CrossRef]
7. Tawalbeh, L.A.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and security: Challenges and solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
8. Lee, A.R.; Kim, B.S.; Jang, J.Y. Risk Analysis for Protecting Personal Information in IoT Environments. *J. Inform. Technol. Ser.* **2016**, *15*, 41–62.
9. Sivaraman, V.; Gharakheili, H.H.; Vishwanath, A.; Boreli, R.; Mehani, O. Network-level security and privacy control for smart-home IoT devices. In Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 19–21 October 2015; pp. 163–167.
10. Williams, M.; Nurse, J.R.; Creese, S. The perfect storm: The privacy paradox and the Internet-of-Things. In Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 644–652.
11. Barth, S.; de Jong, M.D.; Junger, M.; Hartel, P.H.; Roppelt, J.C. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telemat. Inform.* **2019**, *41*, 55–69. [CrossRef]
12. Xu, H.; Luo, X.R.; Carroll, J.M.; Rosson, M.B. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decis. Support Syst.* **2011**, *51*, 42–52. [CrossRef]
13. Alam, M.M.; Malik, H.; Khan, M.I.; Pardy, T.; Kuusik, A.; Le Moullec, Y. A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access* **2018**, *6*, 36611–36631. [CrossRef]
14. Yao, L.; Sheng, Q.Z.; Benatallah, B.; Dustdar, S.; Wang, X.; Shemshadi, A.; Kanhere, S.S. WITS: An IoT-endowed computational framework for activity recognition in personalized smart homes. *Computing* **2018**, *100*, 369–385. [CrossRef]
15. Sutanto, J.; Palme, E.; Tan, C.H.; Phang, C.W. Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Q.* **2013**, *37*, 1141–1164. [CrossRef]
16. Cenfetelli, R.T. Inhibitors and enablers as dual factor concepts in technology usage. *J. Assoc. Inf. Syst.* **2004**, *5*, 472–492. [CrossRef]
17. Cenfetelli, R.T.; Schwarz, A. Identifying and testing the inhibitors of technology usage intentions. *Inform. Syst. Res.* **2011**, *22*, 808–823. [CrossRef]
18. Kim, M.S.; Kim, S. Factors influencing willingness to provide personal information for personalized recommendations. *Comput. Hum. Behav.* **2018**, *88*, 143–152. [CrossRef]
19. Usak, M.; Kubiatko, M.; Shabbir, M.S.; Viktorovna Dudnik, O.; Jermsittiparsert, K.; Rajabion, L. Health care service delivery based on the Internet of things: A systematic and comprehensive study. *Int. J. Commun. Syst.* **2020**, *33*, e4179. [CrossRef]
20. Vandecasteele, B.; Geuens, M. Motivated consumer innovativeness: Concept, measurement, and validation. *Int. J. Res. Mark.* **2010**, *27*, 308–318. [CrossRef]
21. Zhao, L.; Lu, Y.; Gupta, S. Disclosure intention of location-related information in location-based social network service. *Int. J. Electron. Comm.* **2012**, *16*, 53–89. [CrossRef]
22. Li, Y.J.; Kenrick, D.T.; Griskevicius, V.; Neuberg, S.L. Economic decision biases and fundamental motivations: How mating and self-protection alter loss aversion. *J. Pers. Soc. Psychol.* **2012**, *103*, 550–561. [CrossRef]
23. Fritz, T.; Huang, E.M.; Murphy, G.C.; Zimmermann, T. Persuasive technology in the real world: A study of long-term use of activity sensing devices for fitness. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, ON, Canada, 26 April–1 May 2014; pp. 487–496.
24. Meyer, J.; Wasmann, M.; Heuten, W.; El Ali, A.; Boll, S.C. Identification and classification of usage patterns in long-term activity tracking. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, USA, 6–11 May 2017; pp. 667–678.
25. Garg, R. An analysis of (non-) use practices and decisions of internet of things. In Proceedings of the IFIP Conference on Human-Computer Interaction, Paphos, Cyprus, 2–6 September 2019; Springer: Cham, Switzerland, 2019; pp. 3–24.
26. Pavlou, P.A. State of the information privacy literature: Where are we now and where should we go? *MIS Q.* **2011**, *35*, 977–988. [CrossRef]
27. Norberg, P.; Horne, D.; Horne, D. The privacy paradox: Personal information disclosure intentions versus behaviors. *J. Consum. Aff.* **2007**, *4*, 100–126. [CrossRef]
28. Taddicken, M. The 'Privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of Self-Disclosure. *J. Comput-Mediat. Comm.* **2014**, *19*, 248–273. [CrossRef]
29. Aguirre, E.; Roggeveen, A.L.; Grewal, D.; Wetzels, M. The personalization-privacy paradox: Implications for new media. *J. Consum. Mark.* **2016**, *33*, 98–110. [CrossRef]
30. Guo, X.; Zhang, X.; Sun, Y. The privacy–personalization paradox in mHealth services acceptance of different age groups. *Electron. Commer. R. A* **2016**, *16*, 55–65. [CrossRef]

31. Sheng, H.; Nah, F.F.H.; Siau, K. An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns. *J. Assoc. Inf. Syst.* **2008**, *9*, 344–376. [CrossRef]
32. Kim, M. The Impacts of Privacy Rules on Users' Perception on Internet of Things (IoT) Applications: Focusing on Smart Home Security Service. Master's Thesis, Graduate School of UNIST, Ulsan, Korea, 2017.
33. Wang, T.; Duong, T.D.; Chen, C.C. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *Int. J. Inform. Manag.* **2016**, *36*, 531–542. [CrossRef]
34. Herzberg, F. *One More Time: How do You Motivate Employees*; The Leader Manager: New York, NY, USA, 1986.
35. Agarwal, R.; Prasad, J. A conceptual and operational definition of personal innovativeness in the domain of information technology. *Inform. Syst. Res.* **1998**, *9*, 204–215. [CrossRef]
36. Rogers, E.M. *Diffusion of Innovations*, 4th ed.; Free Press: New York, NY, USA, 1995.
37. Vinodh, K.; Mathew, S.K. Web personalization in technology acceptance. In Proceedings of the 2012 4th International Conference on Intelligent Human Computer Interaction (IHCI), Kharagpur, India, 27–29 December 2012; pp. 1–6.
38. Hwang, J.; Park, S.; Kim, I. Understanding motivated consumer innovativeness in the context of a robotic restaurant: The moderating role of product knowledge. *J. Hosp. Tour. Manag.* **2020**, *44*, 272–282. [CrossRef]
39. Reinhardt, R.; Gurtner, S. Differences between early adopters of disruptive and sustaining innovations. *J. Bus. Res.* **2015**, *68*, 137–145. [CrossRef]
40. Esfahani, M.S.; Reynolds, N. Impact of consumer innovativeness on really new product adoption. *Mark. Intell. Plan.* **2021**, *39*, 589–612. [CrossRef]
41. Awad, N.F.; Krishnan, M.S. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Q.* **2006**, *30*, 13–28. [CrossRef]
42. Phelps, J.; Nowak, G.; Ferrell, E. Privacy concerns and consumer willingness to provide personal information. *J. Public Policy Mark.* **2000**, *19*, 27–41. [CrossRef]
43. Samuelson, W.; Zeckhauser, R. Status quo bias in decision making. *J. Risk Uncertain.* **1988**, *1*, 7–59. [CrossRef]
44. Smith, H.J.; Milberg, J.S.; Burke, S.J. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Q.* **1996**, *20*, 167–196. [CrossRef]
45. Garg, R.; Kim, J. An exploratory study for understanding reasons of (Not-) using internet of things. In Proceedings of the Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; pp. 1–6.
46. Wu, L.; Li, J.Y.; Fu, C.Y. The adoption of mobile healthcare by hospital's professionals: An integrative perspective. *Decis. Support Syst.* **2011**, *51*, 587–596. [CrossRef]
47. Yan, Y.; Huang, C.; Wang, Q.; Hu, B. Data mining of customer choice behavior in internet of things within relationship network. *Int. J. Inform. Manag.* **2020**, *50*, 566–574. [CrossRef]
48. Chung, T.; Rust, R.; Wedelm, M. My mobile music: An adaptive personalization system for digital audio players. *Mark. Sci.* **2009**, *28*, 52–68. [CrossRef]
49. Goswami, S.; Chandra, B. Convergence Dynamics of Consumer Innovativeness Vis-á-Vis Technology Acceptance Propensity: An Empirical Study on Adoption of Mobile Devices. *IUP J. Mark. Manag.* **2013**, *12*, 63–87.
50. Kwon, O.; Choi, K.; Kim, M. User acceptance of context-aware services: Self-efficacy, user innovativeness and perceived sensitivity on contextual pressure. *Behav. Inform. Technol.* **2007**, *26*, 483–498. [CrossRef]
51. Venkatraman, M.P. The impact of innovativeness and innovation type on adoption. *J. Retail.* **1991**, *67*, 51–67.
52. Sung, J.; Jo, J. The influence of perceived risk and consumer innovativeness on intention to use of internet of things service. *J. Theor. Appl. Inform. Technol.* **2018**, *96*, 1008–1017.
53. Sweeney, J.; Soutar, G. Consumer perceived value: The development of a multiple item scale. *J. Retail.* **2001**, *77*, 203–220. [CrossRef]
54. Voss, K.E.; Spangenberg, E.R.; Grohmann, B. Measuring the Hedonic and Utilitarian Dimensions of Consumer Attitude. *J. Mark. Res.* **2003**, *40*, 310–320. [CrossRef]
55. Alexander, D.L.; Lynch, J.G.; Wang, Q. As Time Goes By: Do Cold Feet Follow Warm Intentions for Really New Versus Incrementally New Products? *J. Mark. Res.* **2008**, *45*, 307–319. [CrossRef]
56. Vallerand, R.J. Toward a hierarchical model of intrinsic and extrinsic motivation. *Adv. Exp. Soc. Psychol.* **1997**, *29*, 271–360.
57. Ahn, M.; Kang, J.; Hustvedt, G. A model of sustainable household technology acceptance. *Int. J. Consum. Stud.* **2016**, *40*, 83–91. [CrossRef]
58. Paivio, A. *Images in Mind: The Evolution of a Theory*; Harvester Wheatsheaf: New York, NY, USA, 1991.
59. Brown, S.A.; Venkatesh, V. Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle. *MIS Q.* **2005**, *29*, 399–426. [CrossRef]
60. Roehrich, G. Consumer innovativeness: Concepts and measurements. *J. Bus. Res.* **2004**, *57*, 671–677. [CrossRef]
61. Tian, K.T.; Bearden, W.O.; Hunter, G.L. Consumers' Need for Uniqueness: Scale Development and Validation. *J. Consum. Res.* **2001**, *28*, 50–66. [CrossRef]
62. Simonson, I.; Nowlis, S.M. The Role of Explanations and Need for Uniqueness in Consumer Decision Making: Unconventional Choices Based on Reasons. *J. Consum. Res.* **2000**, *27*, 49–68. [CrossRef]

63. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet users information privacy concerns: The construct, the scale, and causal model. *Inform. Syst. Res.* **2004**, *15*, 336–355. [CrossRef]
64. Lee, A.R.; Ahn, H.Y. Fintech users' information privacy concerns and user resistance: Investigating the interaction effect with regulatory focus. *J. Korea Inst. Inform. Secur. Crypt.* **2016**, *26*, 209–226. [CrossRef]
65. Lowry, P.B.; Cao, J.; Everard, A. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *J. Manag. Inform. Syst.* **2011**, *27*, 163–200. [CrossRef]
66. Zhou, T. The effect of perceived justice on LBS users' privacy concern. *Inform. Dev.* **2016**, *32*, 1730–1740. [CrossRef]
67. Zhou, T.; Li, H. Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Comput. Hum. Behav.* **2014**, *37*, 283–289. [CrossRef]
68. Cho, H.; Lee, J.S.; Chung, S. Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Comput. Hum. Behav.* **2010**, *26*, 987–995. [CrossRef]
69. Xu, H.; Teo, H.H.; Tan, B.C.; Agarwal, R. The role of push-pull technology in privacy calculus: The case of location-based services. *J. Manag. Inform. Syst.* **2009**, *26*, 135–174. [CrossRef]
70. Smith, H.J.; Dinev, T.; Xu, H. Information privacy research: An interdisciplinary review. *MIS Q.* **2011**, *35*, 989–1016. [CrossRef]
71. Business Insider Intelligence. Many People still See Smart Home Voice Assistants as a Novelty. Available online: https://www.businessinsider.com/voice-assistants-novelty-2017-1/ (accessed on 1 April 2021).
72. Aldossari, M.Q.; Sidorova, A. Consumer acceptance of Internet of Things (IoT): Smart home context. *J. Comput. Inform.Syst.* **2020**, *60*, 507–517. [CrossRef]
73. Graeber, D. *Toward an Anthropological Theory of Value: The False Coin of Our Own Dreams*; Palgrave: New York, NY, USA, 2001.
74. Boztepe, S. User value: Competing theories and models. *Int. J. Des.* **2007**, *1*, 55–63.
75. Park, J.H.; Ryoo, H.Y. User Value Factors of Internet of Things (IoT) Service. *J. HCI Soc. Korea* **2016**, *11*, 23–30. [CrossRef]
76. Haynes, S.N.; Richard, D.; Kubany, E.S. Content validity in psychological assessment: A functional approach to concepts and methods. *Psychol. Assessment.* **1995**, *7*, 238–247. [CrossRef]
77. Komiak, S.Y.; Benbasat, I. The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Q.* **2006**, *30*, 941–960. [CrossRef]
78. Bhattacherjee, A. Understanding information systems continuance: An expectation-confirmation model. *MIS Q.* **2001**, *25*, 351–370. [CrossRef]
79. Chin, W.W.; Marcolin, B.L.; Newsted, P.R. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and voice mail emotion/adoption study. *Inform. Syst. Res.* **2003**, *14*, 189–217. [CrossRef]
80. Gefen, D.; Straub, D.; Boudreau, M.C. Structural equation modeling and regression: Guidelines for research practice. *Commun. Assoc. Inform. Syst.* **2000**, *4*, 1–79. [CrossRef]
81. Hess, T.J.; Fuller, M.; Campbell, D.E. Designing interfaces with social presence: Using vividness and extraversion to create social recommendation agents. *J. Assoc. Info. Syst.* **2009**, *10*, 889–919. [CrossRef]
82. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
83. Hair, J.F.; Anderson, R.E.; Tatham, R.L.; Black, W.C. *Multivariate Data Analysis with Readings*, 5th ed.; Macmillan: New York, NY, USA, 1998.
84. Podsakoff, P.M.; Organ, D.W. Self-reports in organizational research: Problems and prospects. *J. Manag.* **1986**, *12*, 531–544. [CrossRef]
85. Keil, M.; Tan, B.C.Y.; Wei, K.K.; Saarinen, T.; Tuunainen, V.; Wassenaar, A. A Cross-cultural Study on Escalation of Commitment Behavior in Software Projects. *MIS Q.* **2000**, *24*, 299–325. [CrossRef]
86. Lee, A.R.; Kim, K.K. Customer benefits and value co-creation activities in corporate social networking services. *Behav. Inform. Technol.* **2018**, *37*, 675–692. [CrossRef]
87. Phang, C.W.; Kankanhalli, A.; Sabherwal, R. Usability and sociability in online communities: A comparative study of knowledge seeking and contribution. *J. Assoc. Inf. Syst.* **2009**, *10*, 721–747. [CrossRef]
88. SmartPLS. Available online: https://www.smartpls.com/documentation/videos/pls-mga-pls-multi-group-analysis (accessed on 21 August 2021).
89. Xu, H.; Gupta, S. The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electron. Mark.* **2009**, *19*, 137–149. [CrossRef]
90. Low, S.; Ullah, F.; Shirowzhan, S.; Sepasgozar, S.M.; Lin Lee, C. Smart digital marketing capabilities for sustainable property development: A case of Malaysia. *Sustainability* **2020**, *12*, 5402. [CrossRef]
91. Cirillo, F.; Gómez, D.; Diez, L.; Maestro, I.E.; Gilbert, T.B.J.; Akhavan, R. Smart city IoT services creation through large-scale collaboration. *IEEE Internet Things J.* **2020**, *7*, 5267–5275. [CrossRef]