



Article

Unravelling the Effects of Privacy Policies on Information Disclosure: Insights from E-Commerce Consumer Behavior

Seung Jun Baek and Hong Joo Lee *

Department of Business Administration, The Catholic University of Korea, Bucheon 14662, Republic of Korea; icehund@naver.com

* Correspondence: hongjoo@catholic.ac.kr

Abstract: The aim of this study was to explore the influence of a personal information agreement on customers' information disclosure behavior. By integrating the existing privacy calculus theory, we sought to understand customer behavior in the context of encountering a personal information agreement and to provide insights into the efficacy of a company's privacy policy. Our findings reveal that upon encountering a personal information agreement, customers perceive both a privacy retention period policy and privacy information sharing policy. We discovered that both policies significantly influence the perception of privacy benefits, but only the privacy information sharing policy impacts the perception of privacy risk. Furthermore, while privacy benefits were found to dictate information disclosure behavior in the context of a personal information agreement, perceptions of privacy risk did not significantly affect this behavior.

Keywords: personal information agreement; privacy calculus; privacy paradox; information disclosure behavior; privacy policy



Academic Editor: Zorica Bogdanović

Received: 4 November 2024

Revised: 6 March 2025

Accepted: 6 March 2025

Published: 11 March 2025

Citation: Baek, S.J.; Lee, H.J.

Unravelling the Effects of Privacy Policies on Information Disclosure: Insights from E-Commerce Consumer Behavior. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 49. <https://doi.org/10.3390/jtaer20010049>

Copyright: © 2025 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license

(<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the rise of the Fourth Industrial Revolution and artificial intelligence (AI), activities involving the analysis of users' personal information to provide new services or increase corporate profits through analyzed data have become increasingly prevalent [1,2]. On the other hand, as companies utilize customers' personal information for various analytics and services, there is a growing concern regarding potential violations of customer privacy [3–6]. As digital transformation shifts offline activities to the online realm, customers are increasingly prompted to input their personal information into websites and app services [7]. Customers frequently provide their personal information not only for services they are already using but also for those they may be unfamiliar with, often as part of the membership or purchase process. When registering with a well-known company, customers can decide whether to input their personal information based on their existing perception or image of the company. However, when signing up for a new, lesser-known service, customers must make this decision solely based on the information provided by the company, as they lack any prior knowledge of the company.

Customers have two ways to familiarize themselves with the company's customer privacy policy and can decide whether to provide personal information based on it. The first source is the contents of 'the personal information agreement', which appears on the consent screen before entering personal information. The second source is the contents of 'the Privacy Policy on the website' provided at the bottom of the homepage. Customers should derive the company's privacy policy from these two pieces of information. The

privacy policy on the homepage is accessible only to those who voluntarily choose to read it. Often lengthy, complex, and legally oriented, it poses challenges for the average customer who may not be particularly interested in deciphering its contents. On the other hand, the personal information agreement is presented during the consent stage before entering personal information. The content of this notification is simpler than the privacy policy on website, offering customers information that is easier to understand than the company's comprehensive privacy policy.

In various studies examining factors influencing personal information disclosure behavior, privacy calculus, which interprets such behavior as a choice made by the information subject considering the benefits and risks involved, has been widely utilized [8–10]. These studies have been conducted with the anticipation that individuals' perceived benefits and risks would vary depending on the nature of the service.

Moreover, previous research on privacy policy has explored variations in how customers perceive the comprehensiveness of privacy policy and how this perception influences their intention to provide personal information or use the service, as well as how the wording of the privacy policy on homepage contributes to such perceptions [11–15]. Hence, it has not been feasible to ascertain the influence of customers' perception of the privacy agreement on their behavior at the moment of actual privacy provision. This study concentrates on addressing this issue and aims to investigate the influence of the perception of the privacy policy, as outlined in the personal information agreement, on personal information disclosure behavior. Specifically, numerous information providers furnish subscribers' personal information to third parties to offer convenient services [16]. They often maintain policies to retain personal information for a designated period even after the user unsubscribes, or to continue utilizing acquired content even if the personal information is deleted [17]. Hence, this study aims to assess the impact of the privacy retention period and the privacy information sharing policies on personal information disclosure behavior.

This study examines how customers perceive privacy agreements and how their willingness to disclose personal information varies in response to different privacy agreement contents, using privacy calculus theory as a theoretical framework. An experiment is conducted to test our research hypotheses. The personal information agreement, which customers need to review and agree to during membership registration for the provision of personal information, is displayed in a manner that varies according to the situation, ensuring that customers are informed about the company's privacy policy. To simulate a scenario where a customer encounters an unfamiliar company, we assumed a situation in which a customer signs up for registration at a small online shopping mall, where a corresponding personal information collection agreement is presented. We aim to determine whether customers recognize how the company manages the provision and retention of personal information based on the content of the agreement in this scenario and whether their behavior in providing personal information changes accordingly. This experiment seeks to assess the influence of variations in the privacy information sharing and retention period policy, as outlined in the company's personal information agreement, on customers' behavior in providing personal information. The objective is to establish a foundation for the company to use as a reference when formulating policies for processing personal information.

Compared to previous studies, this study has the following distinctions. Firstly, unlike previous studies grounded in privacy calculus theory, which surveyed customers by recalling the reasons for their behavior, this study employs the personal information agreement that customers must confirm during the registration process as an experimental environment to validate their behavior. Secondly, we expand the current model of privacy calculus theory by incorporating antecedent variables related to the privacy policy and

examining how they influence personal information disclosure behavior. This theoretical extension helps us understand how specific aspects of privacy policies affect users' cost-benefit calculations. Thirdly, while previous research has primarily focused on comprehensive website privacy policies, our study specifically examines the more immediate and accessible personal information agreement that users encounter during the signup process. This focus is particularly relevant as users increasingly engage with unfamiliar services in the digital landscape. Lastly, in the current landscape, where service provision through the extensive analysis of customer personal information using big data and AI is prevalent, this study provides timely insights into how general users perceive and respond to the personal information consent processes when interacting with unfamiliar services.

2. Literature Review

2.1. The Privacy Calculus Theory

The privacy calculus theory is a conceptual framework used to explain users' behavior in providing personal information. It has been extensively applied in prior studies to illustrate that users engage in a cost-benefit analysis, comparing the advantages and risks associated with disclosing personal information when utilizing a service [8,9,18]. Drawing from the privacy calculus theory, studies have investigated whether actual users engage in a cost-benefit analysis to determine whether to provide personal information.

Laufer and Wolfe termed the "calculus of behavior," which refers to individuals' assessment of the consequences of their information disclosure [19]. Culnan and Armstrong introduced the concept of privacy calculus, asserting that when the benefits of providing customer information outweighs the associated risks, customers are more likely to engage in a transaction by providing information [20]. Subsequently, Culnan and Bies delved into the implementation methods within organizations and transactions, building upon the foundational concept of privacy calculus [21].

In the literature, positive and negative factors are frequently considered together to discern the impacts on privacy disclosure behavior. Numerous research efforts have highlighted the role of perceived privacy benefits as a key motivator for individuals' willingness to disclose personal information [9,18,22]. Conversely, a separate strand of research has focused on privacy concerns, rather than privacy risks, as a deterrent in privacy-related decision-making processes [8,22,23]. In the context of this study's experimental framework, we have incorporated privacy risk as a significant variable. We argue that the situational variability of privacy risk makes it a more suitable choice for our investigation compared to privacy concerns, which may be more static and inherent to individuals.

Among the previous studies, some have made significant contributions by extending the model, identifying antecedents that influence privacy benefits and privacy risks in specific situations. For instance, Duan and Deng analyzed how antecedents such as personal innovativeness, perceived ease of use, and trust influence perceived benefits and perceived privacy risks in contact tracing apps adoption [24]. Xu et al. incorporate compensation, industry self-regulation, and government regulation [18]. Kim and Kim include institutional trust for considering perceived privacy control [25]. Sah and Jun demonstrated that privacy awareness serves as an important antecedent variable affecting both privacy benefit and privacy risk in IoT services [10]. Miltgen and Smith investigated how perceptions of privacy benefits, risks, and trust can influence the withholding or falsification of personal information [26]. Schomakers et al. extend its application beyond information disclosure to technology acceptance, demonstrating that individuals' willingness to accept and use smart technologies is determined by weighing the perceived benefits of the technology against privacy concerns [2].

2.2. Privacy Policy

Different policies govern how companies process and manage personal information. However, as users cannot directly access a company's internal regulations, such as the personal information internal management plan or information protection regulations, research on privacy policies has been conducted through surveys to gauge how customers perceive these policies [11,13,14,27].

Wu et al. revealed that effectively communicating access, security, and enforcement in the privacy policy can mitigate privacy concerns, while a well-communicated notice, access, and security can boost privacy trust [15]. Kim and Oh discovered that privacy policies can impact both privacy trust and privacy risk, subsequently affecting intentions to provide personal information [11]. In this study, the survey items were adapted to the consent context by drawing reference from the measures used in these studies.

Analyses of the influence of privacy policy awareness on privacy risk, privacy concerns, and privacy trust have yielded mixed results across various studies. Chang et al., Kim and Oh, and Wu et al. found that awareness of privacy policies reduced privacy risk [11,15,28]. Conversely, Min and Hwang and Park and Kim observed that awareness of privacy policies heightened privacy risk or privacy concerns [13,14]. A similar disparity was noted regarding privacy trust. Chang et al., Esmaeilzadeh, Kim and Oh, and Lee et al. observed that awareness of privacy policies elevated privacy trust, while Min and Hwang found that it decreased privacy trust [11–13,28,29].

This discrepancy can be attributed to the dual impact of privacy policies. Initially, raising awareness of the privacy policy informs customers about the company's personal information processing, simultaneously increasing privacy concerns while diminishing privacy trust. Studies conducted by Min and Hwang, Park and Kim, Yang reported that policy disclosure led to heightened privacy concerns or risks [13,14,30]. These studies incorporated privacy policy awareness as one of several factors influencing privacy concerns or risks. The survey questions also encompassed experiences with privacy breaches, potentially causing the processing of personal information itself to be perceived as a risk.

Conversely, Kim and Oh revealed that transparent disclosure of how a company manages personal information can mitigate privacy concerns and bolster privacy trust [11]. Likewise, Lee et al. uncovered that privacy policies had a positive impact on increasing privacy trust [12]. Furthermore, Wu et al., who segmented privacy policies into distinct elements, observed that raising awareness about choice, security, and regulation reduced privacy concerns [15]. We can anticipate similar outcomes when examining how the scope of personal information sharing policy and the personal information retention period policy are perceived in this experimental scenario.

2.3. Privacy Control

Previous research has utilized survey-based approaches to explore how the perception of data subjects having control over their personal information influences various factors, including privacy concerns, privacy risks, privacy benefits, and personal information disclosure behavior. The perception of having control over privacy influences privacy concerns, subsequently impacting personal information disclosure behavior [14,23,31,32]. Xu et al. also observed that the perceived usefulness of privacy policies can lead to a higher perception of privacy controls, subsequently reducing privacy concerns [33]. Chang et al. also found that privacy control has a positive effect on trust [28]. Dimodugno et al. and Mutimukwe et al. also included privacy controls and privacy concerns in their model to see the impact [34,35].

Other studies have incorporated privacy controls as a variable. For instance, in a study concerning home delivery services, Lim determined that privacy controls were influenced

by perceived knowledge competence and privacy attitudes, subsequently influencing privacy protection behaviors [36]. Yu et al. explored the privacy paradox on Facebook and established that privacy controls exerted a negative influence on privacy concerns, acting as a deterrent to usage intention [37]. They concluded that heightened perceived privacy controls decreased privacy concerns and resulted in higher usage intentions. Anic et al. also found that desire for information control positively influenced online privacy concerns [38].

In studies involving privacy controls, activities that augment privacy controls or perceived privacy controls typically result in reduced privacy concerns. Consequently, in this study, we postulate that if each data subject perceives they can control their privacy in accordance with the company's privacy policy, they will also perceive greater privacy benefits and diminished privacy risks.

3. Research Design

3.1. Research Model and Hypotheses

The research model was organized as illustrated in Figure 1. Consistent with privacy calculus theory, each customer perceives privacy risks and privacy benefits, and these perceptions of privacy risks and benefits exert an influence on information disclosure behavior [8]. In this study, we devised a model rooted in privacy calculus theory, wherein perceived privacy risks and privacy benefits influence personal information disclosure behavior. In the context of personal information collection, our research model encompasses the notion that the level of the privacy retention period policy and privacy information sharing policy, which govern the handling of personal information on the website, impact the perception of privacy risks and privacy benefits.

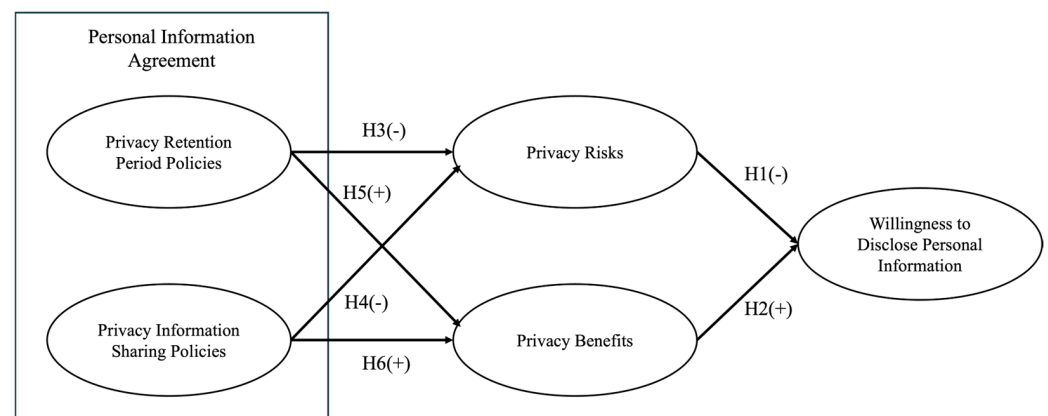


Figure 1. Research model.

Through the research model, we can discern how the content of the personal information agreement provided by the company influences the willingness to disclose personal information in a scenario where users are required to agree to provide personal information during online shopping mall registration. From the perspective of customers who actively utilize online shopping malls, we can ascertain the influence of the shopping mall's personal information agreement on the perception of privacy risks and benefits. Furthermore, from the company's standpoint, which relies on offering services reliant on personal information provision, the contents of the personal information agreement, specifically the privacy retention period policy and the privacy information sharing policy, can serve as a reference for assessing the company's level of personal information utilization. This assessment can be made by examining how the contents of the personal information agreement influence personal information disclosure behavior.

First, drawing upon privacy calculus theory and previous studies utilizing this framework, we formulated two hypotheses to examine the impact of privacy risk and benefit

perceptions on personal information disclosure behavior within the context of obtaining consent for personal information provision. The research hypotheses involve the impact of privacy risks and privacy benefits on personal information disclosure behavior, as explored in previous studies that have applied the privacy calculus theory [8,23].

The concept of privacy calculus was proposed as a theory that if the benefits of providing customer information are higher than the risks of providing information, people will engage in transactions through information provision, and there have been previous studies discussing implementation methods in organizations and transactions based on the concept of privacy calculus. In addition, the concept of privacy calculus has been extended to demonstrate that the perception of privacy risk has a positive effect on privacy concerns, and privacy concerns have a negative effect on the intention to provide personal information in online transactions [8,20,21]. Additionally, a multitude of survey-based studies have demonstrated that an elevated perception of privacy risk has an adverse impact on personal information provision. This effect extends beyond internet transaction-related personal information provision to encompass personalization services, with privacy risk perception detrimentally influencing customers' information disclosure behavior [9,39,40].

Hence, the hypothesized relationship between privacy risk perception and willingness to disclose personal information is as follows.

H1. *An increased perception of privacy risks will negatively impact the willingness to disclose personal information.*

The theory of privacy calculus considers perceived risk as linked to beliefs regarding the extent of privacy leakage, while perceived benefit pertains to the monetary gain from providing personal information or the provision of a service [9]. If the expectation of benefit or usefulness is high, the desire for acceptance, attitude, or informational behavior also increases [18,41,42]. Accordingly, previous survey-based studies have shown that privacy benefit has a positive effect on personal information disclosure behavior [22,40].

Therefore, the hypothesis regarding the relationship between the perception of privacy benefits and willingness to disclose personal information is as follows.

H2. *An increase in privacy benefits will positively impact the willingness to disclose personal information.*

Drawing from the privacy calculus theory, this study establishes that users' perception of the privacy retention period policy and the privacy information sharing policy, as presented by the service provider in the personal information agreement, significantly influences their perception of privacy risks and benefits, subsequently impacting their personal information disclosure behavior. In this experiment, we manipulated two key elements of the privacy agreement: the privacy retention period and the sharing of personal information to third parties. These factors were organized to represent the privacy retention period policy and the privacy information sharing policy. Hypotheses 3 and 4 were formulated to investigate how the perception of the privacy retention period policy and the privacy information sharing policy affects privacy risk.

The analysis of the impact of perceived privacy policy on privacy risk or privacy concerns has yielded varying results across different studies. In this study, we hypothesize that awareness of a privacy policy reduces privacy risk, as observed in studies conducted by Kim and Oh and Wu et al. [15,25]. Unlike previous studies, Min and Hwang, Park and Kim, and Yang, in which awareness of privacy policy increased privacy concerns, this study uses an experimental setting where customers are exposed to a personal information agreement [13,14,30]. Through this experimental design, we aim to examine how the presence of

a clear privacy policy, rather than the mere fact of personal information processing, affects perceived privacy risk.

On the other hand, previous studies have shown that transparent disclosure of how a company handles personal information can reduce privacy concerns. Studies that have broken down privacy policies into elements have also demonstrated that recognizing choice, security, and enforcement can reduce privacy concerns [11,15,28]. We can expect similar results in terms of observing how the privacy information sharing policy and privacy retention period policy perform in this experimental situation.

Furthermore, in terms of control, we anticipate that users' perception of privacy risk will decrease when they are provided with more control over the privacy retention period policy and privacy information sharing policy. Previous research has demonstrated that an increase in perceived privacy control is linked to greater engagement in privacy-conscious behaviors, enhanced trust in companies, and an increased willingness to share personal information. Moreover, studies have indicated that heightened awareness of privacy controls diminishes privacy concerns, enhances usage intention, and encourages greater self-disclosure on SNS [36,37,43].

As a result, we hypothesize that granting users the option to delete their personal information upon unsubscribing and opting not to share their personal information externally will negatively impact the perception of privacy risk.

H3. *Perceived shorter personal information retention periods will have a negative effect on perceived privacy risk.*

H4. *Perceived restriction of personal information sharing with third party companies will have a negative effect on perceived privacy risk.*

Next, we formulated Hypotheses 5 and 6 to investigate how perceptions of the privacy retention period policy and privacy information sharing policy affect privacy benefits.

Previous studies on the impact of privacy policy on privacy trust have yielded varied results. We hypothesize that privacy policy awareness increases perceived privacy benefits, which is consistent with previous research that demonstrated its positive effect on privacy trust [11,12,29].

In contrast to the prior study by Min and Hwang, which discovered that awareness of privacy policies resulted in diminished privacy trust, our study employs an experimental setting where users are prompted to confirm the personal information agreement [13]. Given that the processing of personal information is already established, the significance of how personal information is managed is likely to surpass the awareness of its processing, and consequently, a stricter privacy retention period policy and privacy information sharing policy should increase privacy benefits. Moreover, research exclusively focusing on the impact of privacy policies on privacy trust has consistently revealed that such policies boost privacy trust. Likewise, studies dissecting privacy policies into their constituent elements have underscored that elevating awareness of aspects like notice, choice, and security heightens privacy trust [11,12,15,28].

In the context of perceived control, it is observed that users' perceived privacy benefits increase when they are afforded greater control. Similarly, drawing from previous research that affirms a positive impact of increased privacy controls on privacy behavior and the intention to disclose personal information, as well as prior studies indicating that the utilization of privacy controls results in greater self-exposure on SNS, users tend to perceive heightened privacy benefits when they possess control over their data [28,36,43]. Thus, we formulated a hypothesis suggesting that enabling users to delete their personal

information upon unsubscribing and granting them the choice to refrain from external personal information sharing would result in an increased perception of privacy benefits.

Hence, we established two hypotheses to examine how the privacy retention period policy and the privacy information sharing policy impact users' perceived privacy benefits.

H5. *Perceived shorter personal information retention periods will have a positive effect on perceived privacy benefits.*

H6. *Perceived restriction of personal information sharing with third party companies will have a positive effect on perceived privacy benefits.*

3.2. Experimental Design

The variables of privacy risk, privacy benefit, and information disclosure behavior, as presented in Table 1, were developed based on Kim and Kim [23] and Kim and Kim [25]. In the experimental setting, customers will review the personal information agreement, which includes the website's privacy retention period policy and privacy information sharing policy. We adapted the questions from Kim and Oh to measure the perceived policy using the questions in Table 2 [11]. The survey was conducted in Korean for Korean participants, and the survey items were translated into English for this paper.

Table 1. Measures and variables for privacy benefits, privacy risk, and information disclosure behavior.

Variables	Operational Definitions	Measures
Privacy Benefits	The degree of benefit the subject perceives to be derived from providing personal information to the controller	PIT1: Using this internet service is useful to me. PIT2: Using this internet service is worth it to me. PIT3: Using this internet service is helpful to me. PIT4: Using this internet service is beneficial to me.
Privacy Risks	Perceived risk of the subject's behavior regarding the controller's use of personal information	PRI1: I understand that providing my personal information to this internet service involves risks. PRI2: I believe that providing my personal information to this internet service may cause unforeseen problems. PRI3: I think there is a lot of uncertainty (insecurity) in providing personal information to this internet service. PRI4: I believe that providing personal information to this internet service may result in a loss to me. PRI5: I do not believe it is safe to provide personal information to this internet service.
Willingness to Disclose Personal Information	The extent to which the subject is willing to provide personal information to the controller	IPA1: I willingly provide my personal information when requested for the use of this internet service. IPA2: I generally provide personal information when asked for it in order to use this internet service. IPA3: I readily provide my personal information when it is requested for using this internet service. IPA4: I frequently provide personal information when asked for it in order to use this internet service.

Table 2. Measures and variables for privacy policies.

Variables	Operational Definitions	Measures
Privacy Retention Period Policies	Awareness of how long information controllers keep subjects' personal information	PRPP1: I trust that the internet service will take steps to ensure that my personal information is no longer used when I want it to be. PRPP2: When I want, I will be able to have my personal information deleted from this internet service. PRPP3: I believe that this internet service will stop using the data it analyzes about me when I want it to. PRPP4: When I want, I will be able to have this internet service delete the data it analyzed about me.
Privacy Information Sharing Policies	Awareness that information controllers may provide subjects' personal information to external parties	PPCP1: I believe that my personal information will only be utilized by this internet service that I am a member of. PPCP2: I believe that my membership information is only analyzed by this internet service that I am a member of. PPCP3: I think other companies, not the one I signed up with, will not be able to use the information I provided for this internet service. PPCP4: I believe that other companies, not the one I signed up with, will not be able to analyze and utilize the information I provided for this internet service.

As discussed earlier, users of online services provide personal information in accordance with the policies established by the online service provider in order to use the service. Personal information is provided during the signup or usage stage of the service, and users are informed about the specific personal information that will be collected at that point. Consent is obtained from the user if required. In this study, we conduct an experiment in a scenario where users encounter a personal information agreement to observe how the principles of the privacy calculus theory, as discussed in previous studies, manifest themselves in an online shopping environment. To achieve this, the experiment proceeded in the following sequence: firstly, users were presented with a privacy agreement, followed by a survey to assess their comprehension of the agreement, and finally, a survey was conducted to measure their behavior in that context. Lastly, demographic information was collected.

To examine the influence of the privacy retention period policy and the privacy information sharing policy on perceptions of privacy risks and privacy benefits, four distinct personal information agreements were formulated. These, a two by two factorial design, were developed by varying the magnitude with which the privacy retention period policy and the privacy information sharing policy were manipulated. The privacy retention period policy varied between situations, including cases where member information was deleted upon unsubscription and cases where it was retained for a longer duration, while the privacy information sharing policy varied between situations, involving cases where personal information was provided to a third party and cases where it was not. The four types of situations are presented in Table 3.

Table 3. Situations assigned to each user.

Situations	Personal Information Retention	Personal Information Sharing
Situation 1	Deletion upon withdrawal of membership	No provision of personal information to a third party company
Situation 2	Retention for customer convenience even after withdrawal	No provision of personal information to a third party company
Situation 3	Deletion upon withdrawal of membership	Provided to a third party company for product preference research
Situation 4	Retention for customer convenience even after withdrawal	Provided to a third party company for product preference research

The user is presented with one of four different personal information agreements, depending on the situation. In Situation 1, it is stated that the retained data will be destroyed upon withdrawal, and personal information will not be provided to other companies. In Situation 2, it is stated that personal information will not be provided to other companies, which is the same as in Situation 1, but the retained personal information will continue to be kept even after withdrawal. Situations 3 and 4 are the same as Situations 1 and 2 in terms of the change in the privacy retention period policy, except that personal information is provided to other companies.

After viewing the consent for collecting personal information on this screen, respondents are asked to answer 5-point survey questions regarding how they perceive the privacy retention period policy and the privacy information sharing policy presented. They are also asked questions about how they perceive privacy benefits and privacy risks, as well as their personal information disclosure behavior, all on a 5-point scale. Afterwards, they will respond to questions about their demographic information, and the experiment will conclude. The demographic information includes questions about gender, age group, education, and internet usage.

4. Data Analysis

4.1. Data Characteristics

In conducting the research presented in this study, data were collected through online experiments and questionnaires. Upon accessing the site, individuals were greeted with a detailed explanation of the study's purpose, the nature of the information being collected, and assurances of confidentiality and anonymity.

The survey was conducted using a pool of respondents collected from SurveyMonkey's Audience feature, with a sample size of 197 adults. Data analysis was performed using SPSS version 29 and *semnir* library in R for Partial Least Squares Path Modeling. Out of the 197 participants who completed the online experiment, 185 responses were included in the analysis, while 12 responses were excluded due to their insincerity, which could potentially skew the data in one direction. Table 4 shows the demographic characteristics. The response data can be downloaded at: www.mdpi.com/xxx/s1, Table S1: Response Data.

Table 4. Demographic characteristics.

Demographics	Response	Count	Ratio (%)
Gender	male	94	50.8
	female	91	49.2
Age	~19	1	0.5
	20~29	38	20.5
	30~39	57	30.8
	40~49	56	30.3
	50~59	26	14.1
	60~	7	3.8
Education Level	High school diploma or less	23	12.4
	Community college dropout/graduate	23	12.4
	Bachelor's degree program dropout/graduate	122	65.9
	Graduate school dropout/graduate	17	9.2
Internet Usage Level	It is essential to have someone else's help when using the internet.	7	3.8
	I need some assistance from others when using the internet.	8	4.3
	I can use the internet independently.	19	10.3
	I have no trouble using the internet.	73	39.5
	I can help others use the internet.	78	42.2

Respondents were randomly assigned to one of the four situations, and Table 5 shows the distribution of respondents across each situation. After removing outlier responses, the number of responses analyzed for each situation was 46, 51, 52, and 36 for Situations 1 through 4, respectively. The relatively low number of final responses in Situation 4, compared to the other situations, is likely due to the fact that Situation 4 involves retaining personal information for the longest period of time and providing personal information to a third party. Consequently, fewer users who were assigned to this experimental situation completed the survey.

Table 5. The number of respondents for each situation.

Situations	Respondents		Analysis Sample (After Outlier Removal)	
Situation 1	50	25.4%	46	24.9%
Situation 2	54	27.4%	51	27.6%
Situation 3	55	27.9%	52	28.1%
Situation 4	38	19.3%	36	19.5%

4.2. Preliminary Analysis

The research model comprises five latent variables: privacy retention period policy, privacy information sharing policy, privacy benefit, privacy risk, and willingness to disclose personal information, all of which are rated on a scale from 1 to 5. Frequency analysis was performed to calculate the mean, standard deviation, skewness, and kurtosis of the primary variables intended for use in the structural equation model. The stationarity of the data was assessed, and all variables satisfied the assumption of normal distribution, as indicated by skewness values less than 2 and kurtosis values less than 7. The findings of the preliminary analysis have been summarized into Table 6. Furthermore, the reliability

of each latent variable was assessed using Cronbach's alpha, revealing that all five latent variables had acceptable values, ranging from 0.854 to 0.938. These results are presented in Table 7.

Table 6. Descriptive statistics analysis.

Variables		Mean	Standard Deviation	Skewness	Kurtosis
privacy retention period policies	PRPP1	3.01	1.234	−0.091	−1.145
	PRPP2	3.17	1.179	−0.109	−1.064
	PRPP3	2.97	1.242	0.079	−1.157
	PRPP4	3.14	1.224	−0.046	−1.145
privacy information sharing policies	PPCP1	3.22	1.205	−0.236	−1.002
	PPCP2	3.19	1.270	−0.259	−1.111
	PPCP3	3.04	1.257	0.028	−1.163
	PPCP4	3.01	1.223	0.098	−1.093
privacy benefits	PIT1	3.26	0.927	−0.304	0.104
	PIT2	3.17	0.951	−0.277	−0.059
	PIT3	3.44	0.931	−0.424	0.107
	PIT4	3.18	0.918	−0.235	−0.025
privacy risks	PRI1	3.49	0.927	−0.622	0.038
	PRI2	3.55	0.920	−0.834	0.662
	PRI3	3.49	0.841	−0.528	0.219
	PRI4	3.33	0.929	−0.581	0.061
	PRI5	3.41	0.862	−0.322	0.170
willingness to disclose personal information	IPA1	3.05	0.864	−0.207	0.299
	IPA2	3.35	0.814	−0.715	0.418
	IPA3	2.94	0.910	−0.101	−0.179
	IPA4	3.06	0.904	−0.341	−0.201

Table 7. Reliability analysis.

Variables	Cronbach's Alpha	Number of Items
privacy retention period policies	0.929	4
privacy information sharing policies	0.938	4
privacy benefits	0.925	4
privacy risks	0.898	5
willingness to disclose personal information	0.854	4

Table 8 is intended to show the difference in perception in each situation. To confirm that respondents accurately perceived the differences between the situations, we assessed the perceived value of the privacy retention period policy and the perceived value of the privacy information sharing policy in each situation. We then validated these differences using an independent samples *t*-test. The *t*-test was performed by comparing the perception of the privacy retention period policy for Situations 1 and 3 with Situations 2 and 4, where the privacy information sharing policy was manipulated differently. Additionally, we compared the perception of the privacy information sharing policy for Situations 1 and 2 with Situations 3 and 4, where the privacy information sharing policy was manipulated differently. The results shown in Tables 9 and 10 indicate that participants correctly recognize the difference between the situations, and that the difference is statistically significant.

Table 8. Mean for each situation.

Situations	Privacy Retention Period Policies (Mean)	Privacy Information Sharing Policies (Mean)
Situation 1	3.35	3.53
Situation 2	2.76	3.20
Situation 3	3.41	2.94
Situation 4	2.65	2.70

Table 9. T-test results for differences in perceptions of privacy retention period policies.

	Situation	Count	Mean	Standard Deviation	t	p
PRPP	1/3	98	3.38	1.05	4.259 ***	<0.001
	2/4	87	2.72	1.07		

*** $p < 0.001$.**Table 10.** T-test results for differences in perceptions of privacy information sharing policies.

	Situation	Count	Mean	Standard Deviation	t	p
PPCP	1/2	97	3.36	1.02	3.119 **	0.001
	3/4	88	2.84	1.21		

** $p < 0.01$.

For the validity analysis, factor analysis was performed using principal component analysis as the factor extraction method, followed by varimax rotation. As shown in Table 11, the results demonstrate that all five latent variables were accurately factorized.

Table 11. Factor analysis.

Variables		1	2	3	4	5
Privacy retention period policies	PRPP1	−0.076	0.855	0.110	0.208	0.062
	PRPP2	−0.068	0.881	0.207	0.199	0.017
	PRPP3	−0.024	0.808	0.181	0.300	0.129
	PRPP4	−0.077	0.879	0.173	0.219	0.088
Privacy information sharing policies	PPCP1	−0.121	0.294	0.271	0.818	0.078
	PPCP2	−0.188	0.281	0.226	0.822	0.086
	PPCP3	−0.107	0.251	0.207	0.847	0.096
	PPCP4	−0.155	0.218	0.247	0.829	0.142
Privacy benefits	PIT1	−0.077	0.189	0.824	0.265	0.182
	PIT2	−0.024	0.202	0.823	0.235	0.160
	PIT3	−0.056	0.230	0.836	0.204	0.227
	PIT4	−0.008	0.099	0.853	0.190	0.173
Privacy risks	PRI1	0.783	−0.026	−0.131	−0.112	0.023
	PRI2	0.832	−0.046	0.118	−0.099	0.083
	PRI3	0.892	−0.038	−0.019	−0.095	−0.022
	PRI4	0.849	−0.053	0.053	−0.056	0.015
	PRI5	0.826	−0.086	−0.194	−0.106	0.028

Table 11. *Cont.*

Variables		1	2	3	4	5
Willingness to disclose personal information	IPA1	−0.040	0.052	0.238	0.130	0.819
	IPA2	0.146	0.035	0.162	−0.007	0.790
	IPA3	−0.074	0.154	0.133	0.094	0.834
	IPA4	0.082	0.021	0.081	0.105	0.806
Eigenvalue		3.651	3.39	3.306	3.257	2.861
Common variance (%)		17.385	16.144	15.743	15.51	13.623
Cumulative variance (%)		17.385	33.53	49.273	64.783	78.406

The next phase of our analysis focused on examining the integrity of the model's framework. Refer to Table 12 to review the results of model evaluation. The KMO (Kaiser–Meyer–Olkin) measure was found to be 0.869, and Bartlett's test for sphericity yielded a p -value of less than 0.001, confirming the suitability of the factorization model (approximate Chi-square 3410.537/ $p < 0.001$). The results of the confirmatory factor analysis indicated that the paths from the latent variables to the measured variables were all significant at the 0.001 level of significance.

Table 12. Confirmatory factor analysis.

Latent Variables	Observed Variables	Estimate		S.E.	C.R.
		B	β		
Privacy retention period policies	PRPP1	1	0.833		
	PRPP2	1.041	0.908	0.066	15.836 ***
	PRPP3	1.016	0.841	0.073	13.993 ***
	PRPP4	1.093	0.918	0.068	16.112 ***
Privacy information sharing policies	PPCP1	1.014	0.905	0.057	17.877 ***
	PPCP2	1.062	0.9	0.06	17.662 ***
	PPCP3	1.02	0.873	0.061	16.61 ***
	PPCP4	1	0.88		
Privacy benefits	PIT1	1	0.871		
	PIT2	1.002	0.848	0.067	14.961 ***
	PIT3	1.021	0.886	0.063	16.131 ***
	PIT4	0.94	0.822	0.066	14.194 ***
Privacy risks	PRI1	0.967	0.725	0.091	10.598 ***
	PRI2	1.035	0.782	0.089	11.693 ***
	PRI3	1.071	0.885	0.078	13.706 ***
	PRI4	1.082	0.81	0.088	12.241 ***
	PRI5	1	0.807		
Willingness to disclose personal information	IPA1	1	0.836		
	IPA2	0.809	0.717	0.08	10.085 ***
	IPA3	1.005	0.797	0.089	11.349 ***
	IPA4	0.897	0.716	0.089	10.067 ***

*** $p < 0.001$.

The results of the correlation analysis between the latent variables are presented in Table 13. The correlation coefficients between variables did not exceed 0.8. We evaluated the model's convergent and discriminant validity by calculating the Average Variance Extracted (AVE), Rho_A, and Construct Reliability for each latent variable. Convergent validity was confirmed as all five latent variables had an AVE greater than or equal to 0.5 and both Rho_A and composite reliability values greater than or equal to 0.7. Discriminant validity was confirmed based on the Fornell–Larcker criterion, as the square root of AVE was consistently higher than correlations between constructs.

Table 13. Correlation analysis, AVE, and composite reliability.

	PRPP	PPCP	PIT	PRI	IPA	Average Variance Extracted	Rho_A	Composite Reliability
PRPP	0.908 [†]					0.824	0.933	0.929
PPCP	0.566	0.919 [†]				0.844	0.940	0.938
PIT	0.445	0.549	0.904 [†]			0.817	0.929	0.925
PRI	−0.163	−0.287	−0.137	0.844 [†]		0.712	0.917	0.900
IPA	0.214	0.265	0.415	0.026	0.834 [†]	0.695	0.871	0.854

[†] Square root of AVE.

The Variance Inflation Factor (VIF) values ranged from 1.000 to 1.570, indicating that multicollinearity was not an issue. The f^2 effect size shown in Table 14 indicates medium effects (> 0.15) for the relationships between privacy benefits and personal information disclosure behavior, and between privacy information sharing policies and privacy benefits. Small effects were observed in the relationships between privacy information sharing policies and privacy risks, and between privacy retention period policies and privacy benefits.

Table 14. f^2 effect size.

	PIT	PRI	IPA
PRPP	0.040	0.000	-
PPCP	0.193	0.060	-
PIT	-	-	0.156
PRI	-	-	0.007

We concluded that our model has medium prediction power, as approximately 70% (9 of 13) of the indicators showed lower RMSE values compared to the naïve linear regression model [44].

4.3. Structural Model Analysis

The structural model analysis indicates that the privacy retention period policy does not have a significant effect on privacy risks but does have a positive effect on privacy benefits ($\beta = 0.198, p < 0.01$). The privacy information sharing policy has a negative effect on privacy risks ($\beta = -0.287, p < 0.01$) and a positive effect on privacy benefits ($\beta = 0.437, p < 0.001$). Privacy risks show no significant effect on the willingness to disclose personal information, while privacy benefits have a significant positive effect on the willingness to disclose personal information ($\beta = 0.426, p < 0.001$). The R^2 value for privacy benefits was moderate ($R^2 = 0.328$), while the values for privacy risks and the willingness to disclose

personal information were weak ($R^2 = 0.082$ and 0.179 , respectively). Detailed results of the analysis can be found in Tables 15 and 16.

Table 15. Structural model analysis results.

Paths	β	S.E.	t Statistics	p-Value
privacy retention period policies $\rightarrow$ privacy risks	−0.000	0.108	−0.003	0.9976
privacy retention period policies $\rightarrow$ privacy benefits	0.198	0.074	2.683	0.007 **
privacy information sharing policies $\rightarrow$ privacy risks	− 0.287	0.102	−2.815	0.004 **
privacy information sharing policies $\rightarrow$ privacy benefits	0.437	0.072	6.100	0.000 ***
privacy risks $\rightarrow$ willingness to disclose personal information	0.084	0.100	0.840	0.400
privacy benefits $\rightarrow$ willingness to disclose personal information	0.426	0.085	5.006	0.000 ***

** $p < 0.01$, *** $p < 0.001$.

Table 16. Test results of the research model.

	Hypothesis	Test Results
Hypothesis 1	An increased perception of privacy risks will negatively impact the willingness to disclose personal information.	reject
Hypothesis 2	An increase in privacy benefits will positively impact the willingness to disclose personal information.	accept
Hypothesis 3	Perceived shorter personal information retention periods will have a negative effect on perceived privacy risk.	reject
Hypothesis 4	Perceived restriction of personal information sharing with third party companies will have a negative effect on perceived privacy risk.	accept
Hypothesis 5	Perceived shorter personal information retention periods will have a positive effect on perceived privacy benefits.	accept
Hypothesis 6	Perceived restriction of personal information sharing with third party companies will have a positive effect on perceived privacy benefits.	accept

Figure 2 illustrates the relationships between the variables as presented in the above analysis.

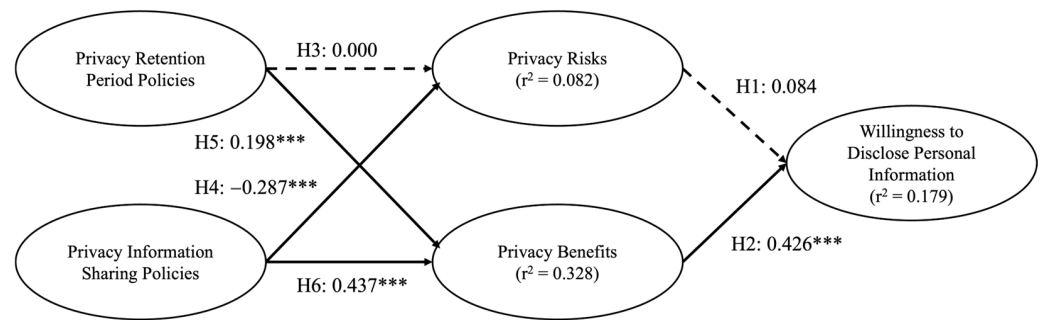


Figure 2. Structural model analysis results. (***) $p < 0.001$.

5. Discussion and Conclusions

5.1. Discussion

The existing research on privacy calculus theory suggests that privacy risk has a negative influence on personal information disclosure behavior, while privacy benefit has a positive influence [8,9,37]. Hypotheses 1 and 2 were formulated to examine whether the principles of the privacy calculus theory apply in our experimental context.

Hypothesis 1, which states that privacy risk has a negative effect on the willingness to disclose personal information, was rejected. In our experiments, it was found that increasing privacy risk had no significant impact on privacy-providing behavior. In other words, participants did not seem to take into account the privacy risk associated with providing personal information in the context of the experimental privacy consent statement. In the context of online shopping malls, the focus of this experiment, it is notable that users opt to disclose personal information despite being conscious of the associated privacy risks, illustrating a form of privacy paradox.

This result contrasts with several prior studies that have confirmed a negative association between privacy risk perception and information disclosure behavior in various online settings [8,18,22,38]. However, our finding aligns with research suggesting that, despite concerns about privacy, individuals often disclose personal information due to other motivating factors, a phenomenon described as the privacy paradox [24,45–47]. For instance, Tsai et al. found that users' privacy concerns did not significantly deter them from making online purchases, even when privacy policies varied [6]. Similarly, Kim et al. demonstrated that privacy risks had no significant impact on the willingness to provide privacy information [9]. In essence, it is a situation characterized by a weak privacy paradox, wherein heightened privacy concerns do not significantly correlate with increased service usage, rather than a strong privacy paradox where rising privacy concerns lead to greater service utilization. In this experiment, we observed that a situation similar to the privacy paradox can arise during the online shopping mall signup process, where users engage in personal information disclosure behavior despite being aware of privacy risks.

Hypothesis 2, which predicts that an increase in privacy benefits will have a positive effect, was found to be statistically significant. This finding is consistent with previous studies that have emphasized the role of perceived benefits in shaping individuals' willingness to disclose personal information [18,22,33]. For example, Xu et al. found that when users perceived tangible benefits, such as financial compensation, they were more likely to share their personal data, despite privacy risks [18]. Likewise, Kim et al. showed that anticipated service-related benefits drive willingness to disclose information in IoT services [9]. Our results reinforce these findings, suggesting that in e-commerce environments, perceived privacy benefits play a more dominant role in shaping disclosure behavior than privacy risks.

Next, we tested Hypotheses 3 and 4 to determine the effects of the privacy retention period policy and the privacy information sharing policy, which were manipulated through the personal information agreement, on participants' perceptions of privacy risk in the experimental situation. We hypothesized that stricter privacy retention period policies and privacy information sharing policies would reduce participants' perceptions of privacy risk.

In the experimental context, it was found that the perception of shorter privacy retention periods did not significantly impact the perception of privacy risk. Therefore, Hypothesis 3 was rejected. Participants did not perceive the retention of information after unsubscribing as a privacy risk. In contrast, we found that restricting the provision of personal information had a negative effect on perceived privacy risk, so Hypothesis 4 was supported. As a result, it appears that the perception of privacy risk is influenced more by the privacy information sharing policy than by the personal information retention period policy.

Considering the hypothesized effect of the privacy information sharing policy on the perception of privacy risk and the effect of the privacy retention period policy on the perception of privacy benefit in the experimental situation, it is somewhat surprising that participants in the experimental situation did not seem to pay close attention to or make the connection between the agreement and privacy risk. Indeed, the results of the *t*-test in the pre-check confirm that participants' perception of the privacy retention period policy varied depending on the situation. It appears more convincing that participants were not concerned in advance about their inability to delete their personal information after unsubscription, given that they were providing their personal information to the online shopping mall for registration. In other words, participants were more concerned about their personal information being provided to a third party at this stage than about how their personal information might be deleted in the future when perceiving privacy risks. It is also possible that they perceived storing their data on the site they chose to sign up for as less risky than providing their data to an unfamiliar third-party company.

We also tested Hypotheses 5 and 6 to assess the impact of the privacy retention period policy and the privacy information sharing policy on perceived privacy benefits. These hypotheses were derived from studies by Kim and Oh, Wu et al., and Lee et al., which emphasized the importance of well-disclosed privacy policies in building trust [11,12,15]. Additionally, they were influenced by research that highlighted the significance of users' perception of privacy control [36,43].

In the experimental context, it was confirmed that reducing the retention period and limiting the sharing of personal information had a positive impact on the perception of privacy benefits, aligning with the hypotheses. Therefore, both Hypotheses 5 and 6 were supported. To put it differently, participants tend to perceive greater privacy benefits when they have control over their personal information as they review the consent to collect personal information. Consequently, perceived privacy benefits contribute to personal information disclosure behavior, so enabling users to restrict the storage and provision of personal information can also lead to personal information disclosure behavior.

In summary, among the privacy policies tested as research hypotheses, the strict establishment of the privacy retention period policy and the privacy information sharing policy has a positive impact on privacy benefits. Moreover, the perception of an increase in privacy benefits is associated with a higher likelihood of personal information disclosure behavior. In our experimental setting, it became evident that privacy policies influence personal information disclosure behavior primarily through their impact on privacy benefits, rather than privacy risks.

5.2. Conclusions

The implications of this study are as follows. Firstly, it examines the applicability of privacy calculus theory in the context of online shopping malls, specifically investigating whether privacy risks and benefits influence the decision to provide personal information. Numerous studies employing privacy calculus theory as a research framework have tested whether users apply this theory when making decisions in various fields. However, our study differs as it employed an experimental methodology using a simulated sign-up scenario in an online shopping mall setting, allowing participants to make real-time decisions rather than relying on the recall process typically used in surveys.

Secondly, our study examined the impact of the personal information agreement on the perception of privacy risk and privacy benefits. In the existing literature, a range of factors has been identified as influencing privacy risk and privacy benefit. Additionally, this study expands upon the existing model by incorporating two new variables from the company's privacy policy: the perception of the privacy retention period policy and the perception of the privacy information sharing policy. These variables are explored for their influence on the perception of privacy risk and privacy benefit.

In our research, we discovered that restricting the provision of personal information more effectively reduces the perception of privacy risk compared to shortening the retention period of personal information. Additionally, we found that both the privacy retention period policy and the privacy information sharing policy influence the perception of privacy benefit. Furthermore, our study succeeded in integrating the content of the personal information agreement as an influential factor within the existing privacy calculus model. Therefore, this study builds upon Gerlach et al. by identifying individuals' perceptions of the privacy agreement and incorporating these perceptions as an independent variable within the privacy calculus theory [48]. Furthermore, in contrast to the approach of Lee and Rha, which utilized the recognition of the privacy agreement for group differentiation, our study demonstrates that the content of the personal information agreement can be effectively expanded as an independent variable [49].

Thirdly, our study identified the factors that exert greater influence on the pathway leading to information disclosure behavior during the stage when customers provide personal information. The experimental results demonstrated that in the context of providing personal information to online shopping malls, privacy benefits can lead to information disclosure behavior, whereas perceived privacy risks do not result in such behavior.

Previous studies employing recall-based surveys to test the theory of privacy calculus have found that both privacy benefits and risks influence personal information disclosure behavior [8,37]. In our experimental setting, we observed that manipulating variables such as the privacy retention period policy and the privacy information sharing policy in the personal information agreement resulted in information disclosure behavior being driven more by privacy benefits than by privacy risks. This implies that at the stage of personal information collection, the perception of privacy benefits takes precedence over concerns regarding privacy risks.

This situation exemplifies a privacy paradox. In our experiments, although users acknowledge privacy risks, these perceptions do not influence their behavior regarding the provision of personal information. Many existing studies on the privacy paradox, which employ surveys, have confirmed its occurrence. Yet, they tend to focus primarily on the varying degrees of the paradox, such as cases where privacy concerns have a significant positive impact on personal information disclosure behavior, and others where the impact is not significant [45,47]. As this study was conducted in an experimental research setting, it is pertinent to consider that the actual decision-making process might differ from that in a recall-based survey.

In practical terms, this study offers guidance for companies on implementing their privacy policies. Our findings indicate that enabling customers to perceive control over their personal information positively affects their privacy benefits, leading to more informed behavior. The analysis of these personal information agreements can serve as a guide for companies aiming to analyze and utilize personal information. It helps in establishing privacy policies concerning the duration of personal information collection and decisions regarding its provision. In an era where the use of personal information is increasingly prevalent, this study offers valuable insights into crafting notices for personal information use and in formulating a company's privacy policy. In other words, by establishing policies that grant customers control over their personal information, it is possible to enhance their willingness to disclose information.

5.3. Limitations and Future Research

While this study offers valuable insights into the impact of personal information agreements on privacy perceptions and willingness to disclose personal information, it also has limitations.

First, regarding the measurement of manipulated variables, instead of using traditional manipulation check questions, we employed full-scale measures to assess participants' perceptions of privacy policy elements. While this approach provides richer insights into how participants interpret these privacy policies, it may not serve as a direct manipulation check.

Second, the uneven distribution of responses across scenarios presents a limitation. Situation 4 had a lower completion rate, likely due to the heightened privacy concerns associated with extended data retention and third-party information sharing. This discrepancy suggests potential response bias, where participants opted out of the study based on their sensitivity to privacy risks. While our analysis maintained statistical adequacy, future studies could address this issue by employing alternative experimental designs, such as ensuring equal sample sizes across conditions or using incentive-based mechanisms to encourage completion.

Third, our choice of SEM over ANOVA for data analysis is another aspect to consider. While ANOVA is commonly used for experimental studies with manipulated variables, we opted for SEM to assess the complex relationships between privacy risk, privacy benefit, and the willingness to disclose personal information. This approach aligns with prior studies using SEM in experimental settings. However, we acknowledge that ANOVA could provide additional insights into direct group differences, and future studies may benefit from a comparative approach using both methods.

Beyond these methodological considerations, this study is also limited to online shopping mall registration contexts, focusing solely on personal information agreements. The results of this study might vary in other industries or in activities beyond membership registration, such as in different contexts of online shopping malls. Additionally, as this study focused solely on manipulating the personal information agreement, the outcomes may differ when considering other aspects of the privacy policy in homepage, where customers can review the processing of their personal information.

Furthermore, within the scope of privacy policies, easily recognizable and measurable elements such as the privacy retention period policy and the privacy information sharing policy were selected as experimental variables in the personal information collection agreement. This experiment, focused on an online shopping mall's membership registration for delivery purposes, did not account for the manipulation of personal information sharing items due to the service's limited nature. However, other services might consider manipulating these variables. Therefore, there is potential to expand the model to include such manipulations.

Additionally, while our finding that privacy risk does not lead to personal information disclosure behavior during the personal information agreement aligns with the privacy paradox, it was not verified using privacy concerns as a metric. Future research could thus explore the impact of privacy concerns in similar experimental contexts.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/jtaer20010049/s1>, Table S1: Response Data.

Author Contributions: Conceptualization, S.J.B. and H.J.L.; methodology, S.J.B. and H.J.L.; software, S.J.B.; formal analysis, S.J.B.; writing—original draft preparation, S.J.B.; writing—review and editing, H.J.L.; supervision, H.J.L.; and funding acquisition, H.J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2017S1A5A2A01025690).

Institutional Review Board Statement: Not applicable.

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

Data Availability Statement: The original contributions presented in this study are included in the Supplementary Material. Further inquiries can be directed to the corresponding author.

Acknowledgments: This study is based on the first author's doctoral dissertation.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Jung, H.; Park, S.; Hyun, D. A priority analysis of policy implementation tasks for the revitalization of the big data industry: Based on the analysis of policy priority using AHP. *Korean J. Broadcast. Telecommun. Stud.* **2021**, *35*, 283–313. [\[CrossRef\]](#)
2. Schomakers, E.-M.; Lidynia, C.; Ziefle, M. The Role of Privacy in the Acceptance of Smart Technologies: Applying the Privacy Calculus to Technology Acceptance. *Int. J. Hum.-Comput. Interact.* **2022**, *38*, 1276–1289. [\[CrossRef\]](#)
3. Bamberger, K.A.; Egelman, S.; Han, C.; On, A.E.B.; Reyes, I. Can You Pay For Privacy? Consumer Expectations and the Behavior of Free and Paid Apps. *Berkeley Technol. Law J.* **2020**, *35*, 327–365. [\[CrossRef\]](#)
4. Choi, B.; Wu, Y.; Yu, J.; Land, L. Love at First Sight: The Interplay Between Privacy Dispositions and Privacy Calculus in Online Social Connectivity Management. *J. Assoc. Inf. Syst.* **2018**, *19*, 124–151. [\[CrossRef\]](#)
5. Hirschprung, R.; Toch, E.; Bolton, F.; Maimon, O. A methodology for estimating the value of privacy in information disclosure systems. *Comput. Hum. Behav.* **2016**, *61*, 443–453. [\[CrossRef\]](#)
6. Tsai, J.Y.; Egelman, S.; Cranor, L.; Acquisti, A. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Inf. Syst. Res.* **2011**, *22*, 254. [\[CrossRef\]](#)
7. Al-Natour, S.; Cavusoglu, H.; Benbasat, I.; Aleem, U. An empirical investigation of the antecedents and consequences of privacy uncertainty in the context of mobile apps. *Inf. Syst. Res.* **2020**, *31*, 1037–1063. [\[CrossRef\]](#)
8. Dinev, T.; Hart, P. An Extended Privacy Calculus Model for E-Commerce Transactions. *Inf. Syst. Res.* **2006**, *17*, 61–80. [\[CrossRef\]](#)
9. Kim, D.; Park, K.; Park, Y.; Ahn, J. Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Comput. Hum. Behav.* **2019**, *92*, 273–281. [\[CrossRef\]](#)
10. Sah, J.; Jun, S. The Role of Consumers' Privacy Awareness in the Privacy Calculus for IoT Services. *Int. J. Hum.-Comput. Interact.* **2024**, *40*, 3173–3184. [\[CrossRef\]](#)
11. Kim, J.; Oh, D. The Effect of Privacy Policy Awareness on the Willingness to Provide Personal Information in Electronic Commerce. *Inf. Syst. Rev.* **2016**, *18*, 185–207. [\[CrossRef\]](#)
12. Lee, K.; Koo, C.; Lee, D. An Empirical Study of Trust Building through Privacy Policies in Sharing Economy: Accumulated Effects of Cultural Background. *J. Korea Serv. Manag. Soc.* **2017**, *18*, 315–340. [\[CrossRef\]](#)
13. Min, H.; Hwang, G. The effect of Privacy Factors on the Provision Intention of Individual Information from the SNS Users. *J. Digit. Converg.* **2016**, *14*, 1–12. [\[CrossRef\]](#)
14. Park, C.; Kim, J. An Empirical Research on Information Privacy Concern in the IoT Era. *J. Digit. Converg.* **2016**, *14*, 65–72. [\[CrossRef\]](#)
15. Wu, K.; Huang, S.Y.; Yen, D.C.; Popova, I. The effect of online privacy policy on consumer privacy concern and trust. *Comput. Hum. Behav.* **2012**, *28*, 889–897. [\[CrossRef\]](#)

16. Jai, T.C.; King, N.J. Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *J. Retail. Consum. Serv.* **2016**, *28*, 296–303. [\[CrossRef\]](#)
17. Hong, J. A Study on the Institutional Plan on Financial Consumer Protection in the Case of Unfair Settlement due to Information Leak: Focusing on the Contents of the Comprehensive Digital Finance Innovation Plan. *Korean J. Ind. Secur.* **2020**, *10*, 89–110. [\[CrossRef\]](#)
18. Xu, H.; Teo, H.; Tan, B.C.Y.; Agarwal, R. The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *J. Manag. Inf. Syst.* **2009**, *26*, 135–173. [\[CrossRef\]](#)
19. Laufer, R.S.; Wolfe, M. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *J. Soc. Issues* **1977**, *33*, 22–42. [\[CrossRef\]](#)
20. Culnan, M.J.; Armstrong, P.K. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organ. Sci.* **1999**, *10*, 104–115. [\[CrossRef\]](#)
21. Culnan, M.J.; Bies, R.J. Consumer Privacy: Balancing Economic and Justice Considerations. *J. Soc. Issues* **2003**, *59*, 323–342. [\[CrossRef\]](#)
22. Al-Jabri, I.M.; Eid, M.I.; Abed, A. The willingness to disclose personal information: Trade-off between privacy concerns and benefits. *Inf. Comput. Secur.* **2019**, *28*, 161–181. [\[CrossRef\]](#)
23. Kim, J.; Kim, J. A Study on the Internet User's Economic Behavior of Provision of Personal Information: Focused on the Privacy Calculus, CPM Theory. *J. Inf. Syst.* **2017**, *26*, 93–123. [\[CrossRef\]](#)
24. Duan, S.X.; Deng, H. Exploring privacy paradox in contact tracing apps adoption. *Internet Res.* **2022**, *32*, 1725–1750. [\[CrossRef\]](#)
25. Kim, S.; Kim, J. Impact of Privacy Concern and Institutional Trust on Privacy Decision Making: A Comparison of E-Commerce and Location-Based Service. *J. Korea Ind. Inf. Syst. Res.* **2017**, *22*, 69–87. [\[CrossRef\]](#)
26. Miltgen, C.L.; Smith, H.J. Falsifying and withholding: Exploring individuals' contextual privacy-related decision-making. *Inf. Manag.* **2019**, *56*, 696–717. [\[CrossRef\]](#)
27. Rodríguez-Priego, N.; van Bavel, R.; Monteleone, S. The disconnection between privacy notices and information disclosure: An online experiment. *Econ. Politica J. Anal. Institutional Econ.* **2016**, *33*, 433–461. [\[CrossRef\]](#)
28. Chang, Y.; Wong, S.F.; Libaque-Saenz, C.F.; Lee, H. The role of privacy policy on consumers' perceived privacy. *Gov. Inf. Q.* **2018**, *35*, 445–459. [\[CrossRef\]](#)
29. Esmaeilzadeh, P. The impacts of the privacy policy on individual trust in health information exchanges (HIEs). *Internet Res.* **2020**, *30*, 811–843. [\[CrossRef\]](#)
30. Yang, S.J. Impacts of Female College Students' Perceived Security on Attitude Toward SNS after Reading Privacy Policies of SNS. *J. Consum. Cult.* **2018**, *21*, 113–131. [\[CrossRef\]](#)
31. Cheng, Z.; Li, K.; Teng, C. Understanding the influence of privacy protection functions on continuance usage of push notification service. *Aslib J. Inf. Manag.* **2022**, *74*, 202–224. [\[CrossRef\]](#)
32. Feng, Y.; Xie, Q. Privacy Concerns, Perceived Intrusiveness, and Privacy Controls: An Analysis of Virtual Try-On Apps. *J. Interact. Advert.* **2019**, *19*, 43–57. [\[CrossRef\]](#)
33. Xu, H.; Luo, X.; 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. [\[CrossRef\]](#)
34. Dimodugno, M.; Hallman, S.; Plaisent, M.; Bernard, P. The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach. *J. Phys. Conf. Ser.* **2021**, *2090*, 012017. [\[CrossRef\]](#)
35. Mutimukwe, C.; Kolkowska, E.; Grönlund, Å. Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Gov. Inf. Q.* **2020**, *37*, 1–13. [\[CrossRef\]](#)
36. Lim, S.H. An Empirical Study on the Privacy Protection Intention and Behavior of B2C Delivery Services User: TRA (Theory of Reasoned Action) Approach. *Korea Logist. Rev.* **2020**, *30*, 101413. [\[CrossRef\]](#)
37. Yu, J.H.; Lee, A.R.; Kim, K.K. Investigating the Privacy Paradox in Facebook Based on Dual Factor Theory. *Knowl. Manag. Res.* **2016**, *17*, 17–47. [\[CrossRef\]](#)
38. Anic, I.; Škare, V.; Kursan Milaković, I. The determinants and effects of online privacy concerns in the context of e-commerce. *Electron. Commer. Res. Appl.* **2019**, *36*, 100868. [\[CrossRef\]](#)
39. 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. [\[CrossRef\]](#)
40. Lee, E.; Kim, H.; Kim, J.; Koo, C. Exploring Factors Affecting Attitude toward Disclosure of Personal Information in Restaurants during the COVID-19 Pandemic. *J. Tour. Sci.* **2021**, *45*, 123–147. [\[CrossRef\]](#)
41. Dinev, T.; Albano, V.; Xu, H.; D'Atri, A.; Hart, P. Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective. In *Advances in Healthcare Informatics and Analytics*; Gupta, A., Patel, V., Greenes, R., Eds.; Springer International Publishing: Berlin, Germany, 2016; Volume 19, pp. 19–50. [\[CrossRef\]](#)
42. Li, H.; Sarathy, R.; Xu, H. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decis. Support Syst.* **2011**, *51*, 434–445. [\[CrossRef\]](#)

43. Kim, G. A Moderating Effect of Use of Interaction Privacy Controls on the Relationship between Privacy Concerns and Self-disclosure. *J. Korea Soc. Comput. Inf.* **2020**, *25*, 235–241. [[CrossRef](#)]
44. Hair, J.; Hult, G.; Ringle, C.; Sarstedt, M.; Danks, N.; Ray, S. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*; Springer: Cham, Switzerland, 2021.
45. Choi, H.; Lee, M.; Lee, H. Is There a Privacy Paradox in the Online Purchasing Context?: The Study on the Effects of Privacy Concern and Online Purchasing Behavior. *J. Prod. Res.* **2019**, *37*, 1–13. [[CrossRef](#)]
46. Gonçalves, R.B.; De Figueiredo, J.C.B. Effects of perceived risks and benefits in the formation of the consumption privacy paradox: A study of the use of wearables in people practicing physical activities. *Electron. Mark.* **2022**, *32*, 1485–1499. [[CrossRef](#)]
47. Shin, I. Difference of Privacy Paradox on Open and Closed SNS. *Informatiz. Policy* **2020**, *27*, 72–91. [[CrossRef](#)]
48. Gerlach, J.; Widjaja, T.; Buxmann, P. Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *J. Strat. Inf. Syst.* **2015**, *24*, 33–43. [[CrossRef](#)]
49. Lee, J.; Rha, J. Effects of Informed Consent on Young Consumers' Willingness to Provide Personal Information and Intention to Use Location-based Mobile Commerce. *Consum. Policy Educ. Rev.* **2016**, *12*, 1–24. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.