A STUDY ON THE INFLUENCE OF PRIVACY CONCERNS ON USERS' PURCHASE INTENTION IN E-COMMERCE ENVIRONMENT

WANG ZHEN
6417195009

AN INDEPENDENT STUDY SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF BUSINESS ADMINISTRATION
GRADUATE SCHOOL OF BUSINESS
SIAM UNIVERSITY
2025

A STUDY ON THE INFLUENCE OF PRIVACY CONCERNS ON USERS' PURCHASE INTENTION IN E-COMMERCE ENVIRONMENT

WANG ZHEN

This Independent Study Has Been Approved as a Partial Fulfillment of the Requirements for the Degree of Master of Business Administration

Advisor......Chao Qiu......
(Assoc.Prof.Dr.Qiu Chao)

Date: ....13../.....8..../..........2025

....
(Associate Professor Dr. Jomphong Mongkhonvanit)
Dean, Graduate School of Business

Date.......17..../.....9...../..2025..............

Title: A Study on the Influence of Privacy Concerns on Users' Purchase Intention in E-commerce Environment

Researcher: WANG ZHEN

Degree: Master of Business Administration

Major: International Business Management

Advisor: ....Chao Qin........

(Assoc.Prof.Dr.Qiu Chao)

........13 / 8 / 2025........

ABSTRACT

With the proliferation of e-commerce, concerns over users' personal information privacy have become increasingly prominent. In this context, privacy concern has emerged as a key psychological factor influencing users' online behavior. However, prior research has often treated privacy concern as a single construct, without fully exploring its multidimensional effects. This study aimed to investigate how different dimensions of privacy concern, namely, collection, errors, improper access, and secondary use, affect users' perceived risk and, in turn, their purchase intention on e-commerce platforms. Additionally, the study examined the mediating role of perceived risk and the moderating effect of privacy policy. The specific objectives were: 1) To examine the impact of privacy concern on perceived risk. 2) To examine the effect of perceived risk on purchase intention. 3) To examine the influence of privacy concern on purchase intention. 4) To explore the mediating role of perceived risk in the relationship between privacy concern and purchase intention. 5) To explore the moderating effect of privacy policy on the relationship between privacy concern and perceived risk.

To achieve these objectives, the study adopted a quantitative research method by designing and administering a structured questionnaire. The measurement items were based on validated scales, utilizing a 5-point Likert scale. Data were analyzed using SPSS and AMOS, employing structural equation modeling to test the hypothesized relationships and validate the research model. This study selected users of e-commerce platforms as the research subjects. After excluding invalid and incomplete responses, a total of 390 valid questionnaires were collected, yielding an effective response rate of 56%.

The findings indicate that all four dimensions of privacy concern significantly increase perceived risk, which in turn negatively influences purchase intention. Perceived risk also plays a mediating role in the relationship between privacy concern and purchase intention. Moreover, privacy policy partially moderates the impact of improper access and secondary use on perceived risk, but has no significant moderating effect on the dimensions of collection and errors.

Keyword: privacy concern, purchase intention, perceived risk

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to my advisor for his invaluable guidance, support, and encouragement throughout my Independent Study. His insightful comments and constructive criticism have significantly improved the quality of my work.

Additionally, I am grateful to Associate Professor Dr. Jomphong Mongkhonvanit, Dean, Graduate School of Business, for his support and encouragement throughout my studies. His dedication to the graduate program and commitment to excellence have inspired me to strive for academic excellence.

Finally, I would like to extend my appreciation to all the faculty members and staff of Siam University who have contributed to my growth and development as a student. Their unwavering support and encouragement have been a source of inspiration and motivation to me.

WANG ZHEN

DECLARATION

I, WANG ZHEN, hereby declare that this Independent Study entitled “A Study on the Influence of Privacy Concerns on Users' Purchase Intention in E-commerce Environment” is an original work and has never been submitted to any academic institution for a degree.

(WANG ZHEN)
Feb 20, 2025

CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1 Introduction

1.1 Background of the Study

The emergence of e-commerce has driven societal economic growth while providing people with a faster and more convenient way to access products and services. Online shopping via e-commerce platforms eliminates time and location constraints, gradually replacing traditional offline shopping and becoming the preferred choice for consumers. E-commerce refers to a business model where users conduct online transactions and electronic payments via the internet (Smith & Johnson, 2022). Its rise and development are closely tied to the rapid advancement of internet technology.

Unlike traditional offline shopping, all transaction records on e-commerce platforms are stored in the platform’s database, and the subsequent use of this data remains uncertain. This uncertainty triggers users' concerns about their personal privacy. To enhance profitability and meet diverse consumer demands, e-commerce platforms intentionally collect and analyze users' personal data, providing merchants with diversified sales channels and assisting them in developing targeted marketing strategies (Lee et al., 2021). Additionally, platforms aim to improve service quality, enhance user experience, and increase customer retention. However, some unethical merchants excessively collect and misuse personal data, leading to frequent privacy breaches and unprecedented threats to users' personal information (Wang & Zhang, 2023).

In reality, most privacy leaks occur because platforms share stored user data with third parties, resulting in financial and reputational losses for users and even disrupting their daily lives (Chen et al., 2020). Cases of fraudsters impersonating e-commerce customer service representatives have become increasingly common, further eroding user trust in e-commerce platforms and highlighting growing privacy concerns.

Privacy security threats are not entirely imperceptible. When signs of potential privacy risks emerge, users can often perceive these threats to some extent. Once users sense a risk, they are likely to take measures to mitigate or avoid potential harm, minimizing possible losses (Kim & Park, 2022). Some users may even choose to delete their platform accounts, which contradicts e-commerce’s goal of high-quality development and hinders its future growth.

According to the China Internet Network Information Center (CNNIC) report, as of December 2023, China’s internet penetration rate reached 73%, with 43.2% of individuals aged 60 and above being active internet users (CNNIC, 2024). In the internet era, older adults have not been left behind—many can now independently engage in digital activities such as e-travel, QR-code payments, and online searches (Liu et al., 2023). Currently, internet adoption continues to accelerate. Given China's national context and the big data era, exploring the mediating role of perceived risk between privacy concerns and purchase intention is a question of significant theoretical and practical value (Zhou & Li, 2021).

1.2 Questions of the Study

1. How does privacy concern affect consumers' perceived risk?

2. What is the effect of perceived risk on consumers' purchase intention?

3. How does privacy concern influence consumers' purchase intention?

4. Does perceived risk mediate the relationship between privacy concern and purchase intention?

5. Does privacy policy moderate the relationship between privacy concern and perceived risk?

1.3 Objectives of the Study

1. To examine the impact of privacy concern on perceived risk.

2. To examine the effect of perceived risk on purchase intention.

3. To examine the influence of privacy concern on purchase intention.

4. To explore the mediating role of perceived risk in the relationship between privacy concern and purchase intention.

5. To explore the moderating effect of privacy policy on the relationship between privacy concern and perceived risk.

1.4 Scope of the Study

This study placed privacy concerns in the context of e-commerce, and took users who use e-commerce platforms to make purchases as the research objects. This study explored the relationship between four variables: privacy concern, perceived risk, privacy policy and user purchase intention. A quantitative research method was employed to test the proposed hypotheses. Data were collected using an online structured questionnaire distributed through digital platforms such as Wenjuanxing. After eliminating invalid and incomplete responses, a total of 390 valid samples were obtained. The collected data were analyzed using SPSS and AMOS to examine the measurement and structural models.

1.5 Significance of the Study

Theoretical significance: In the context of the big data era, the two-way flow of information between users and e-commerce platforms is inevitable. However, a frequent phenomenon is that users' personal information is extensively utilized by e-commerce merchants without their knowledge, significantly threatening the confidentiality of their private data. Ideally, e-commerce platforms should collect and analyze users' personal information for the purpose of social innovation and value creation. Yet, due to technological limitations and profit-driven motives, users' private data is frequently leaked. Whether in the collection or analysis of internet-based information, disclosed personal data faces risks such as Improper exposure and undisclosed usage, leaving users' privacy unprotected and substantially increasing their level of privacy concern.

While existing literature includes numerous studies on purchase intention, research on the relationship between privacy concern and purchase intention remains scarce. This study addresses fundamental theoretical issues in e-commerce by reviewing and synthesizing literature on key concepts including privacy concern, perceived risk, purchase intention, and privacy policies. By directly examining the correlation between privacy concern and purchase intention, this study enhances the focus of its research, aiming to advance theoretical understanding in areas such as privacy concern and purchase intention. Additionally, this study is grounded in prospect theory and technology.

Practical significance: In the context of modern technological advancement playing a pivotal role, China's e-commerce research has evolved from a follower to a leader in the field. Within the current e-commerce landscape, privacy issues have emerged as one of the most significant concerns accompanying the development of information technology. The recurring incidents of privacy breaches have brought the importance of personal data protection to the forefront of public attention. The improper collection and misuse of personal information by certain unethical e-commerce merchants has further reinforced the critical need for privacy protection. This study focuses on privacy issues among e-commerce platform users, seeking to understand their awareness of privacy concerns and provide explanatory insights into their subsequent behaviors. The research aims to help e-commerce platforms accurately comprehend the concept of user privacy concerns, thereby enabling both platform operators and public policy makers to develop marketing strategies and regulatory policies that genuinely address user needs, based on a profound understanding of user psychology and behavioral patterns.

1.6 Definition of Key Terms

Privacy Concern: Refers to the consumer’s worry or apprehension regarding the security and protection of personal information during collection, storage, processing, and use. It reflects the sensitivity towards potential privacy violations.

Perceived Risk: Represents the level of uncertainty and potential negative consequences (such as information leakage, identity theft, or privacy breaches) that consumers believe may arise from privacy issues.

Privacy Policy: In this study, the privacy policy is defined as the directive statement by e-commerce platforms on how they collect and use users' private information. It serves as a mandatory regulation established by the platform to protect personal privacy information.

Purchase Intention: Denotes the consumer’s willingness or inclination to buy a particular product or service. It is considered an important predictor of actual purchase behavior.

Collection: Refers to the actions taken by enterprises or organizations to gather consumers’ personal information, including the type, scope, and frequency of the data collected. Excessive or non-transparent data collection may increase consumers’ perceived risk.

Errors: Refers to inaccuracies or mistakes occurring during the collection, processing, or storage of data, which may lead to misinformation or data breaches, thereby increasing perceived risk.

Improper Access: Refers to unauthorized entities accessing, stealing, or exploiting consumers’ personal information. Such behavior directly raises consumers’ concerns about information security.

Secondary Use: Refers to the use of consumers’ personal information for purposes other than the original intent at the time of collection. This behavior may trigger concerns about information diffusion and privacy invasion.

Chapter 2 Literature Review

2.1 Privacy Concern

The concept of privacy concern was initially proposed to measure the level of users' concern about personal privacy information when using e-commerce platforms. Westin (1968) was the first to introduce the concept of privacy concern, defining it as an individual’s subjective perception of fairness in a particular context. Castaneda and Montoro (2007) believed that at any stage of a transaction, information provided by consumers in advance, newly emerged transaction information, and related information could all trigger a series of privacy issues, such as how the information is utilized and whether it is obtained and used by third parties. This phenomenon may lead to the emergence of consumer privacy concerns. Phelps et al. (2001) further refined the concept by describing privacy concern as consumers’ attention to the degree of control over their personal information, as well as their concern about others collecting and using their private data.

At present, the concept of privacy concern has not yet reached a consensus in academia. Many scholars define privacy concern based on the specific research context, while some directly equate privacy concern with privacy awareness. This study, based on the e-commerce environment, describes privacy concern as users' level of concern regarding the scope and subsequent use of their personal information collected when registering, using, and making purchases on e-commerce platforms.

Many scholars have developed a series of privacy concern scales to measure the level of "privacy concern" among users. There are numerous studies on the dimensional division of privacy concerns, but the specific content of these divisions varies. Stone et al. (1983) divided the privacy concern scale into four dimensions to measure the degree of concern individuals within an organization have about their private information: collection, storage, use, and dissemination. Over time, as research on privacy concerns deepened, scholars gradually developed privacy concern scales with multiple dimensions. Based on the frequency of use and the corresponding research content, the Concern for Information Privacy (CFIP) scale and the Internet Users' Information Privacy Concerns (IUIPC) scale are frequently applied and considered mature scales. Smith et al. (1996), from a strategic theory perspective, developed a privacy concern scale that includes four dimensions: collection, Improper secondary use, improper access, and errors. The initial purpose of this scale was to measure the level of privacy concern among employees in enterprises. The specific definitions of the dimensions are as follows: collection refers to the amount of personal privacy information collected by e-commerce platforms; Improper secondary use refers to the use of user privacy information in the database by e-commerce platforms without user consent or authorization; improper access refers to the acquisition or use of personal privacy information disclosed by users by parties other than the e-commerce platform without user authorization; errors refer to inaccuracies in the collected user privacy information due to the platform's lack of security and privacy protection measures. The dimensional division of this scale is widely used in academia, but compared to the online environment, it is more suitable for traditional offline shopping environments. Sheehan and Hoy (2000), based on the internet environment, divided the privacy scale into five dimensions: cognitive, use, sensitivity, familiarity, and compensation.

Subsequently, based on the CFIP scale, Stewart and Segars (2002) improved and supplemented it by proposing a second-order factor and empirically testing it, addressing the incompleteness of the first-order factor model in describing variables and enhancing the operability of the scale. Malhotra et al. (2004) pointed out that the realization of transactions between platforms and users is based on a certain contractual relationship established between them, and using this as a theoretical foundation, they developed the IUIPC scale based on the CFIP scale. This scale divides privacy concerns into three dimensions: collection, control, and awareness. The IUIPC scale was proposed to measure the level of user privacy concern in the internet environment and remains highly relevant and operable today. The specific explanations of the IUIPC scale dimensions are as follows: "collection" determines the extent to which people are concerned about others possessing their private information relative to the value obtained; "control" represents the individual's belief in their right to decide whether to accept or reject others' decisions regarding the processing of their private information; "privacy awareness" refers to consumers' awareness of the information privacy statements provided by organizations. In the IUIPC scale, the collection dimension is generally considered the starting point for measuring privacy concerns, while the control dimension is the most important. The IUIPC model is more concise and widely applicable than other models, making it frequently used in academia. Tavani (2007) argued that the control dimension is the most important in the expression of privacy concerns, including control over choice, permission, and correction. Choice refers to the right to choose the context in which information is provided, to set public or private settings, and to control others' access to personal information. Permission refers to the right to refuse others' access to personal information. Correction refers to the right to amend disclosed personal information. Hong and Thong (2013), from the perspective of interpersonal interaction in multidimensional development theory, integrated the

CFIP scale and the IUIPC scale to form a third-order scale, dividing privacy concerns into six dimensions: collection, secondary use, errors, improper access, control, and awareness. This third-order factor model significantly outperforms the pre-integration data in terms of validity and data fit. Li et al. (2023) divided online users' privacy concerns into three dimensions: collection, control, and understanding. Matzger (2007) first proposed from a legal perspective that the dimensional division of privacy concerns also includes a law enforcement dimension.

The dimensional division of privacy concerns by previous scholars provides a theoretical foundation for subsequent research in different contexts and perspectives. Therefore, this study adopts a classic and basic division, categorizing privacy concerns into four dimensions: collection, errors, improper access, and secondary use. Collection refers to the extent of user information collection by e-commerce platforms. Errors refer to the accuracy of personal information stored in e-commerce platform databases. Improper access refers to the prohibition of third-party access to or sharing of personal information without user consent. Secondary use refers to the prohibition of using user personal information for other purposes without user authorization.

2.2 Perceived Risk

The concept of perceived risk was first introduced in the field of psychology. Bauer (1960) brought the concept of perceived risk from psychology into marketing. He argued that users' sharing of their own information or inadvertent leakage during purchasing behavior could lead to unpredictable losses, and this uncontrollability prompts users to perceive risk. According to his view, after the user's transaction process ends, it is difficult to actively predict subsequent events and their outcomes, and the value brought by the desired products and services is also unknown. Whether the products or services can meet the actual needs of consumers is also uncertain. Therefore, users' purchasing behavior is full of uncertainty, and the concept of risk arises from this unknown. Cox (1964) believed that the factors influencing perceived risk include both psychological and financial aspects of consumers, largely occurring before consumers make a purchase. It is the consumer's choice of the desired product or service, coupled with hesitation, that strengthens the concern about the potential risks of the product or service. Alternatively, after the purchase, if the purchased product or service does not meet the consumer's actual needs or achieve the psychological goal, it results in a perceived sense of loss, which Cox conceptualized. He divided the consumer's shopping behavior into two periods and explained them separately: the perceived risk before shopping stems from the uncertainty of the outcomes during and after the shopping process; the perceived risk after shopping stems from the consumer's subjective sense of loss. Bettman (1973) divided perceived risk into handled risk and inherent risk. He explained them as follows: the perceived risk when consumers purchase a brand is handled risk; the perceived risk hidden behind a certain type of product is inherent risk. When consumers purchase their preferred brand, the inherent risk is relatively low, and they are more likely to make a secure purchase. In the e-commerce environment, the flow of information and the flow of actual value are inconsistent with the traditional purchasing environment, making the relationship between the user and their behavior more ambiguous, thereby generating new unknown perceived risks. As the name suggests, online perceived risk arises because the development of the internet has made consumers perceive risks when shopping online. Another definition states that online perceived risk is the insufficient security of information and the leakage of personal privacy information, generally believed to be caused by the lack of credibility of e-commerce platform merchants. By summarizing the concepts of user perceived risk on the internet, this study identifies three characteristics of perceived risk: online perceived risk originates from traditional perceived risk, but online perceived risk emphasizes subjectivity, and its core content is the uncertainty and loss of the outcome.

Scholars have divided perceived risk into the following dimensions: First, financial risk, which generally refers to consumers' perception of risks related to money or property. In the e-commerce environment, it specifically manifests as the perceived danger during payment. Second, product performance risk, which refers to the hidden dangers of the product or service that consumers intend to purchase to meet their diverse needs. In the e-commerce environment, it is reflected in the platform's reputation; platforms with higher reputations are more likely to gain consumer trust and reduce perceived risk. Third, physical risk, which refers to the perceived risk of damage to the consumer's mental health. Fourth, social risk, which arises from the use of a product or service that negatively affects others in society, causing losses to others. Fifth, psychological risk, which arises from the negative impact on the consumer's self-image after purchasing and using a product or service. Wang and Wang (2013) divided consumers' perceived risk into financial risk, privacy risk, product risk, event risk, and social risk, clarifying the relationship between user perceived risk and purchase intention. Shi (2023) divided perceived risk into functional risk, payment risk, product risk, delivery risk, time risk, and privacy risk. In the e-commerce environment, Cui (2019) divided perceived risk into product risk, financial risk, psychological risk, and system risk. Financial risk, product risk, and information risk are considered the three most common risks when consumers shop online. Product risk is generally considered to be related to the product itself, such as quality issues. Financial risk includes not only risks related to money and property but also risks in the marketing process, such as repeated purchases due to network issues or platform vulnerabilities. Information risk, as the name suggests, is closely related to users' personal privacy information, such as when information provided by users on the internet is obtained by malicious actors for fraudulent purposes. Dong (2007), after summarizing relevant literature, believed that users' perceived risk during online transactions has four dimensions: core service risk of online retailers, accompanying risks of online shopping, personal privacy risk, and product risk.

By summarizing the relevant literature on perceived risk, it is found that the dimensional division of perceived risk reflects both the intrinsic conceptual nature of perceived risk and its impact on people's behavioral intentions. This study mainly studies whether users' privacy concerns in the e-commerce environment can affect their purchase intentions. Therefore, this study studies perceived risk from the perspective of user psychology, treating users' perceived privacy risk as the sole dimension of perceived risk, and incorporating perceived risk as a variable into the model construction.

2.3 Purchase Intention

The concept of purchase intention was first introduced in the field of psychology. Chaiken (1991) was the first to define the concept of purchase intention, arguing that consumers' purchase intention originates from a psychological idea, where they plan the desired product in advance and then proceed to make a purchase. In subsequent research, the definition of consumer purchase intention has been continuously expanded and supplemented by researchers. Dodd et al. (1991) mentioned in his work that purchase intention is the customer's subjective desire to obtain a product. Fishbein (1975) believed that intention is the probability of an individual subjectively performing a specific behavior, and purchase intention is the probability of a customer subjectively performing a purchase behavior. Xue et al. (2022) also pointed out that purchase intention is the consumer's subjective prediction of purchasing a product or service, and when the product satisfies the consumer, the purchase behavior can be realized.

Zeithaml (1988) studied methods for measuring purchase intention from the perspective of perceived value, dividing purchase intention into three dimensions: considering purchase, wanting to purchase, and likely to purchase. Building on this research, Berry and Parasuraman (1996) expanded Zeithaml and Boulding's measurement method, dividing purchase intention into six dimensions: considering purchase, wanting to purchase, likely to purchase, repurchase rate, building platform reputation, and recommending to others. Li et al. (2023) measured privacy concerns by dividing the dimensions of privacy concerns into repurchase rate, active purchase, and recommendation to others. The APCO model combines the antecedents and outcomes of privacy concerns to optimally leverage empirical testing, where antecedents include privacy experience, privacy awareness, individual differences, demographic variables, and cultural environment, and outcomes include behavioral intention, trust, regulations, and perceived risk. The APCO model is suitable for the specific environment of the Internet of Things and is widely used in the field of privacy concern research, serving as one of the foundational models for exploring privacy concerns in the digital economy era.

The occurrence of user purchase behavior is significantly influenced by purchase intention. Generally, user purchase behavior occurs after the user has developed purchase intention, and once purchase intention is formed, it is likely to prompt the user to make a purchase. Due to various influencing factors and constraints in reality, there is often a lack of high consistency between user purchase intention and purchase behavior, making the occurrence of purchase behavior somewhat uncertain. The stronger the user's desire for a product or service, the more money or time they are willing to spend on it, and the more positively purchase intention influences the occurrence of purchase behavior. However, due to the inherent uncertainty of users, purchase intention can also be used as a reflection of user behavior, substituting for behavioral prediction. Bagozzi (1989) also confirmed the unity of intention and behavior. Du et al. (2023) pointed out in her research on behavioral prediction that people's intentions can be included as variables in the research framework.

2.4 Privacy Policies

The development of data technology has increased the demand for personal information by e-commerce platforms to enhance their marketing services. However, users' concerns about platforms collecting their private information often lead them to habitually refuse to disclose their personal data. Strengthening platform self-management is one effective way to protect users' personal information. By formulating rigorous privacy protection policies, platforms can effectively increase users' willingness to protect their privacy.

Privacy policies are documents published online by internet platforms, covering the collection and use of users' personal information, including why, how, and how much information is collected. Privacy policies are also measures to protect users' privacy, serving as safeguards against unlawful infringement of users' private information. Privacy policies should be publicly released, comprehensive, accurate, and easy to understand, clearly stating the platform's responsibilities and obligations, as well as the penalties for violating the policy. This provides effective oversight of how platforms handle users' personal information. Different platforms may use different names for their privacy policies, but the concepts are generally similar, with similar functions. Terms such as privacy clauses, privacy agreements, and privacy statements are often used interchangeably or mixed with privacy policies.

This study uses the term "privacy policy" to describe these documents uniformly, defining a privacy policy as an e-commerce platform's directive statement on how it collects and uses users' private information, serving as a mandatory regulation for protecting personal information.

Privacy policies include six dimensions: transparency, usage restrictions, access, correction, data quality, and security. Based on the principle of fairness, the U.S. federal government divides privacy policy dimensions into notice, choice, access, security, and enforcement. Guo et al. (2021) identified three key dimensions of privacy policies: transparency, control, and protection. Transparency refers to how the privacy policy describes the platform's use of collected user information, clarifying the scope and amount of information collected to ensure users' right to know. Control refers to the degree of control users have over their private information, such as searching, updating, or modifying the information they have disclosed to the platform, as well as the right to decide the scope of information disclosure and selectively disclose information the platform intends to collect. Protection refers to the measures the platform takes to protect user privacy, ensuring the security of users' personal information in the platform's database. Currently, there is no unified standard for the dimensional division of privacy policies. In empirical research, Bansal and Zahedi (2008) divided privacy policy dimensions into users' understanding of the policy and the comprehensiveness of the policy's content. Scholars often measure privacy policies by examining all the clauses related to protecting users' personal information in the platform's online privacy policy. Gao et al. (2023) summarized previous research and divided privacy policies into two dimensions: structural and content dimensions. The structural dimension refers to limiting the scope of information collection and use by the platform, ensuring the quality of information collection through clear explanations, and providing users with accessible channels for reporting issues, simplifying the reporting process, and addressing user complaints promptly. The content dimension refers to the clarity, readability, and comprehensiveness of the privacy policy's content, which enhances users' control over their personal information, increases trust in the platform, reduces privacy concerns, and encourages users to disclose their information to the platform, thereby supporting the platform's technological development. Wang (2019) measured the perceived effectiveness of privacy policies directly as a variable.

This study, from a user psychology perspective, uses privacy policy as a variable to moderate the relationship between privacy concerns and users' perceived risk. Therefore, drawing on Wang's dimensional measurement research, the effectiveness of the privacy policy is included as a single-dimensional variable in the model framework for research and measurement.

2.5 Theoretical Foundations

2.5.1 Prospect Theory

Prospect Theory was first proposed by Kahneman and Tversky (2008). They argued that when individuals are in an uncertain environment, they evaluate perceived value and perceived risk, and based on the evaluation results, their behavioral intentions are influenced, leading to corresponding actions. Prospect Theory provides the following two explanations for the patterns of consumer decision-making behavior: on one hand, potential consumers are accustomed to avoiding risks they face during shopping; on the other hand, by comparing consumers' subjective attitudes toward gains and losses, it is found that consumers pay significantly more attention to losses. From this, it can be concluded that if consumers perceive risks during shopping, and the existence of these risks disrupts the balance between final benefits and costs, they will pay more attention to the risks and attempt to take a series of measures to reasonably and effectively avoid them. The prospect Theory provides a strong foundation for the hypotheses and model construction in this study.

2.5.2 Theory of Reasoned Action

Theory of Reasoned Action (TRA) was proposed by Fishbein and Ajzen in 1975. The theory states that people's attitudes and subjective norms directly influence their behavioral intentions, which in turn lead to certain decision-making behaviors.

From the theoretical model, it can be seen that attitudes and subjective norms can act as mediating variables between the independent variables and individual behavioral intentions. Gao (2022), based on Theory of Reasoned Action, used perceived risk as a mediating variable to confirm the relationship between internal and external factors and customers' purchase intentions. The Theory of Reasoned Action has been widely used in studies of individual consumer behavior, but its premise is based on the assumption of rational individuals, meaning that every individual makes decisions after rational consideration in daily life, which differs from reality.

2.5.3 Theory of Planned Behavior

Theory of Planned Behavior (TPB) was first proposed by Professor Ajzen (1991). The Theory of Planned Behavior emphasizes that individuals' subjective norms, attitudes, and perceived behavioral control directly influence their behavioral intentions, and the occurrence of individual behavior is related to behavioral intentions. Previous research has shown that the Theory of Planned Behavior can effectively predict individuals' behavioral intentions and decision-making behaviors. Liu and Wei (2022) proposed that the Theory of Planned Behavior is highly adaptable for studying user behavioral intentions.

2.6 Conceptual Framework

Regarding research on the impact of user privacy concerns on behavioral intentions, early scholars primarily focused on the field of social networks. The research content rarely considered the role of privacy concerns among e-commerce platform users. This study places privacy concerns in the context of e-commerce environments, exploring the mutual influence mechanisms between user privacy concerns, perceived risk, and purchase intention. It expands on previous research that mainly examined factors such as trust, social support, and perceived value on user purchase intentions, providing a more comprehensive reference for the impact of privacy concerns on the purchase intentions of e-commerce platform users.

Some merchants on e-commerce platforms have attempted to reduce users' privacy concerns by using privacy policies and privacy clauses. The existence of privacy policies can, to some extent, reduce the risk of misuse of users' personal information. Research has shown that the existence and effectiveness of privacy policies are effective institutional mechanisms for reducing user privacy concerns. Therefore, this study introduces privacy policy as a moderating variable to explore whether it plays a significant role in the relationship between privacy concerns and perceived risk.

In summary, this study treats privacy concern as the independent variable, perceived risk as the mediating variable, user purchase intention as the dependent variable, and privacy policy as the moderating variable. It explores the main effect of privacy concern on user purchase intention, the mediating effect of perceived risk on the relationship between privacy concern and purchase intention, and the moderating effect of privacy policy on the relationship between privacy concern and perceived risk. The theoretical model of this study is shown in Figure 2.1.

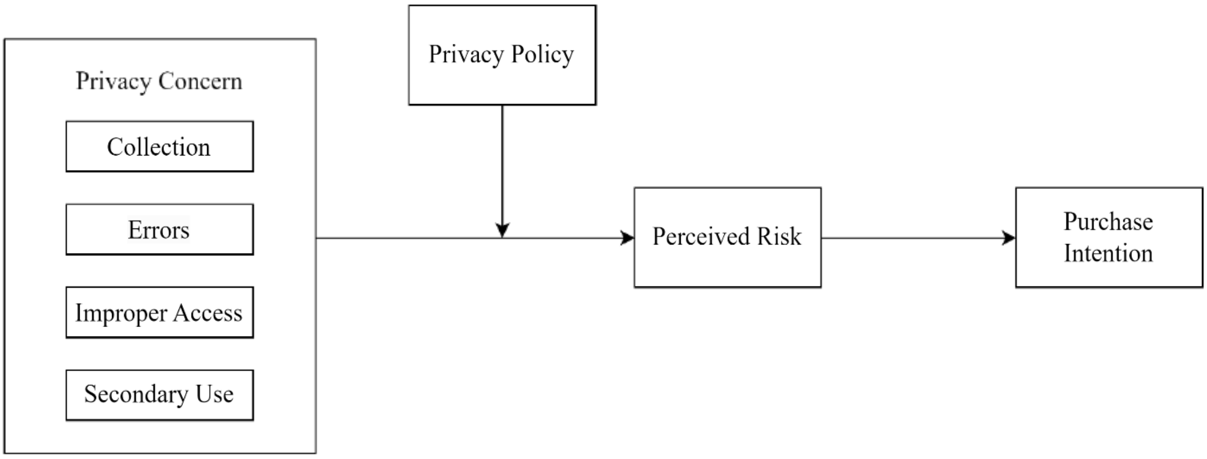

Figure 2.1 Conceptual Framework

Chapter 3 Research Methodology

3.1 Research Design

This study adopted the quantitative research, using a questionnaire survey to collect data. This study positioned privacy concern as the independent variable, perceived risk as the mediating variable, user purchase intention as the dependent variable, and privacy policy as the moderating variable. It explored the effect of privacy concern on user purchase intention, the mediating effect of perceived risk on the relationship between privacy concern and purchase intention, and the moderating effect of privacy policy on the relationship between privacy concern and perceived risk. Appropriate subjects and channels were selected for distribution to validate the rationality of the hypotheses. Using SPSS and AMOS data analysis software, a quantitative analysis was first conducted to explore the reliability of the variables. Subsequently, statistical analysis of the sample data was performed to measure its reliability and validity. Finally, based on the results of the reliability and validity tests, the model's fit was analyzed, along with the examination of mediating and moderating variables, to verify the accuracy of the model and hypotheses.

3.2 Questionnaire Design

This study involves four key variables: privacy concern, perceived risk, privacy policy, and purchase intention. By summarizing relevant literature, a questionnaire was designed and divided into six parts. The first part is the questionnaire introduction, explaining the purpose of the questionnaire. The second part collects basic personal information, including five questions on gender, age, education level, consumption level, and occupation. The third part measures the dimensions and items of privacy concern, including 4 items for collection, 4 items for errors, 3 items for improper access, and 4 items for secondary use. The fourth part includes 4 measurement items for perceived risk. The fifth part includes 4 measurement items for purchase intention. The sixth part includes 4 measurement items for privacy policy. This study selected scales commonly used by scholars and made appropriate adjustments based on the research content. A 5-point Likert scale is used, with scores ranging from 1 to 5: (1) strongly disagree, (2) somewhat disagree, (3) neutral, (4) somewhat agree, and (5) strongly agree. Respondents were asked to rate each item based on their level of agreement. The detailed questionnaire can be found in the appendix. Below is an explanation of the measurement scales for these variables, including the sources of the scales, the dimensional division of the variables, and the specific measurement items for each variable.

(1) Measurement of privacy concern. This study posits that privacy concern refers to users' attention to the extent of online collection of private information by e-commerce platforms and its subsequent use. Drawing on the research designs of Stewart and Segars (2002) and Smith et al. (1996), privacy concern is measured across four dimensions: collection, errors, Improper Access, and secondary use. A total of 15 measurement questions were asked, as shown in Table 3.1.

Table 3.1 Measurement of Privacy Concern

Dimension	No.	Measurement Items	Source
Collection	1	I feel annoyed when e-commerce platforms ask me to provide or allow them to collect my personal information.	Stewart (2002) 、 Smith et al. (1996)
	2	I always consider carefully when e-commerce platforms ask me to provide or allow them to collect my personal information.	
	3	Providing my personal information to different e-commerce platforms makes me uneasy.	
	4	I am concerned that e-commerce platforms collect too much of my personal information.	
Errors	5	E-commerce platforms should take more measures to ensure the accuracy of personal information.	
	6	E-commerce platforms should have better procedures to correct errors in personal information.	
	7	E-commerce platforms should invest more time and effort in verifying the accuracy of personal information in their databases.	
	8	I believe that personal information stored in databases should be double-checked to ensure accuracy.	
Improper Access	9	E-commerce platforms should invest more time and effort to prevent Improper Access to personal information.	
	10	E-commerce platforms should take more measures to prevent Improper users from accessing personal information.	
	11	I believe that databases storing personal information should be protected to prevent Improper Access.	

Secondary Use	12	E-commerce platforms should not sell personal information in their databases to other companies.	
	13	E-commerce platforms should not use personal information for any purpose without user authorization.	
	14	E-commerce platforms should not share user personal information with other companies without user authorization.	
	15	When users provide personal information for a specific purpose, the platform should not use the information for other purposes.	

(2) Measurement of Perceived Risk. This study posits that perceived risk refers to users' perception of the uncertain consequences that may arise from disclosing personal privacy information. Drawing on the research design of Liu and Wang (2018), it includes four measurement items, as shown in Table 3.2.

Table 3.2 Measurement of Perceived Risk

Dimension	No.	Measurement Items	Source
Perceived Risk	16	I believe there is a certain risk in providing personal privacy information to e-commerce platforms.	Liu & Wang (2018)
	17	I believe providing personal privacy information to e-commerce platforms may lead to potential losses.	
	18	I believe providing personal privacy information to e-commerce platforms involves many unexpected issues.	
	19	I believe providing personal privacy information to e-commerce platforms brings a lot of uncertainty.	

(3) Measurement of Purchase Intention. In this study, purchase intention refers to users' inclination to engage in transactions on e-commerce platforms to obtain related services or products. Drawing on the research designs of Kim et al. (2008) and Jarvenpaa et al. (2000), it includes four measurement items, as shown in Table 3.3.

Table 3.3 Measurement of Purchase Intention

Dimension	No.	Measurement Items	Source
Purchase Intention	20	I would recommend this e-commerce platform to my friends.	Kim et al. (2008)
	21	Overall, I am willing to continue using online e-commerce platforms.	
	22	Compared to offline shopping, I prefer purchasing any needed products through online e-commerce platforms.	

	23	If I need a product soon, I might consider purchasing it through an online e-commerce platform.	

(4) Measurement of Privacy Policy. This study posits that a privacy policy is a set of regulations published online by e-commerce platforms to ensure the security of users' disclosed private information. Through the publication of online privacy policies, users can understand the extent to which the platform protects their personal information. The measurement primarily references the research designs of Yuan and Niu (2021) and Gong et al. (2019), including four items. The measurement items are shown in Table 3.4.

Table 3.4 Measurement of Privacy Policy

Dimension	No.	Measurement Items	Source
Privacy Policy	24	I believe that the clauses promised in the privacy policy of the e-commerce platform have been fully implemented.	Yuan & Niu (2021) 、Gong et al. (2019)
	25	I believe that the privacy policy of the e-commerce platform ensures the security of my private information.	
	26	I believe that the privacy policy of the e-commerce platform reduces my sense of privacy risk.	
	27	I believe that the privacy policy of the e-commerce platform is an effective commitment to protecting users' private information.	

3.3 Hypothesis

H1: Privacy concern has a positive impact on perceived risk.

H1a: Collection has a positive impact on perceived risk.

H1b: Errors have a positive impact on perceived risk.

H1c: Improper access has a positive impact on perceived risk.

H1d: Secondary use has a positive impact on perceived risk.

H2: Perceived risk has a negative impact on purchase intention.

H3: Privacy concern has a negative impact on purchase intention.

H3a: Collection has a negative impact on purchase intention.

H3b: Errors have a negative impact on purchase intention.

H3c: Improper access has a negative impact on purchase intention.

H3d: Secondary use has a negative impact on purchase intention.

H4: Perceived risk mediates the relationship between privacy concern and purchase intention.

H4a: Perceived risk mediates the relationship between collection and purchase intention.

H4b: Perceived risk mediates the relationship between errors and purchase intention.

H4c: Perceived risk mediates the relationship between improper access and purchase intention.

H4d: Perceived risk mediates the relationship between secondary use and purchase intention.

H5: Privacy policy moderates the relationship between privacy concern and perceived risk.

H5a: Privacy policy moderates the relationship between collection and perceived risk.

H5b: Privacy policy moderates the relationship between errors and perceived risk.

H5c: Privacy policy moderates the relationship between improper access and perceived risk.

H5d: Privacy policy moderates the relationship between secondary use and perceived risk.

3.4 Sampling and Data Collection

3.4.1 Sampling

This study selected users of e-commerce platforms as the research subjects, primarily based on the following two considerations. On one hand, e-commerce has developed rapidly, with a large user base, and online shopping has largely replaced offline shopping, as people generally fulfill their consumption needs through online purchases. On the other hand, this study explores the relationship between privacy concern and user purchase intention in the context of e-commerce, making e-commerce platform users more representative and allowing for a more intuitive reflection of the survey results' validity. Therefore, this study uses e-commerce platform users as an example to investigate the internal mechanisms and boundary conditions between privacy concerns and user purchase intentions.

3.4.2 Data Collection

The data for this study were collected through online surveys. The survey was distributed and collected via the online platform "Wenjuanxing" (Questionnaire Star), and links were shared on multiple apps such as WeChat, Weibo, and QQ. The survey was promoted across multiple platforms, and respondents were encouraged to share the survey or collaborate with others who had similar needs. The survey period of this study started in November 2024 and ended in June 2025.The survey targeted individuals of different ages, occupations, and consumption levels. A total of 500 questionnaires were distributed, which 109 invalid responses were removed, resulting in 390 valid responses, with a questionnaire validity rate of 78.2%.

3.5 Data Analysis

3.5.1 Descriptive Statistical Analysis

Descriptive statistical analysis involves describing the frequency, mean, and other indicators of the basic information of the survey respondents in the sample data. This study primarily conducted descriptive statistical analysis on gender, age, education level, consumption level, and occupation to gain a preliminary understanding of the basic characteristics of the sample data and to develop an overall understanding of e-commerce platform users.

3.5.2 Reliability and Validity Testing Methods

Reliability reflects the internal consistency and stability of the sample data, while validity is mainly used to test the rationality of the questionnaire structure. Reliability and validity analysis are essential steps in empirical research.

(1) Reliability Testing: This tests whether the collected data are reliable. Currently, Cronbach's Alpha (α) coefficient is commonly used to analyze reliability. The general standards are as follows: if Cronbach's Alpha (α) coefficient < 0.6, the reliability is poor, and some items need to be modified or deleted before further analysis; if 0.6 < Cronbach's Alpha (α) coefficient < 0.7, the reliability is acceptable; if 0.7 < Cronbach's Alpha (α) coefficient < 0.8, the reliability is good; and if Cronbach's Alpha (α) coefficient > 0.8, the reliability is high.

(2) Validity Testing: This tests the extent to which the items in the scale explain the variables, i.e., whether the items in the scale reasonably express the variables. This study primarily uses exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) to test validity.

3.5.3 Correlation Analysis

Correlation analysis is generally used to determine the relationships between multiple variables. Typically, the Pearson coefficient is used to judge the strength and direction of the relationship. A positive coefficient indicates a positive correlation between variables, while a negative coefficient indicates a negative correlation. The closer the absolute value of the coefficient is to 1, the stronger the correlation; conversely, the weaker the correlation. A coefficient of 0.7 and 0.4 serves as a threshold for judging the strength of the correlation: an absolute value greater than 0.7 indicates a strong correlation, between 0.4 and 0.7 indicates a moderate correlation, and between 0.2 and 0.4 indicates a weak correlation.

3.5.4 Regression Analysis

Linear regression, one of the most commonly used regression analysis methods in research, aims to explore the mechanisms of influence between variables, showing how changes in one variable affect another. Key indicators in linear regression include R^2, adjusted R^2, F-value, and VIF. This study used hierarchical regression to test the proposed mediating and moderating variables in the model and further employed the Bootstrap method to verify the accuracy of the mediating effects.

3.6 Reliability and Validity Analysis of the Scale

3.6.1 Reliability Testing

This study used SPSS to conduct reliability testing by calculating Cronbach's α values. As shown in Table 3.5, the Cronbach's α values for the factors of privacy concerns are 0.840, 0.820, 0.803, and 0.812, respectively; the Cronbach's α value for perceived risk is 0.835; for purchase intention, it is 0.825; and for privacy policy, it is 0.854. All values meet the standard of being greater than 0.8. The reliability of the scale used in this study is high, indicating that the measurement model has high reliability. Therefore, the data obtained are suitable for further analysis.

Table 3.5 Scale Reliability Results

Variable	Factor	Number of Items	Cronbach's α
Privacy Concern	Collection	4	0.840
	Errors	4	0.820
	Improper Access	3	0.803
	Secondary Use	4	0.812
Perceived Risk		4	0.835
Purchase Intention		4	0.825
Privacy Policy		4	0.854

3.6.2 Validity Testing

This study used SPSS to conduct validity analysis on the sample. Data with KMO values greater than 0.7 and Bartlett's sphericity test significance of 0.000 are considered to pass the test. The results show that the KMO coefficients for privacy concern, perceived risk, purchase intention, and privacy policy are 0.89, 0.805, 0.804, and 0.818, respectively, all greater than 0.7, with p-values of 0.000, less than 0.001. The variance explanation rates are 67.51%, 66.97%, 65.67%, and 69.63%, respectively, all exceeding

60%. The variables in the scale used in this study all pass the test, indicating good item validity and meeting the design standards of mature scales.

Table 3.6 Percentage and KMO Values of the Scale

Variable	Variance Explanation Rates	KMO value
Privacy Concern	67.51%	0.890***
Perceived Risk	66.97%	0.805***
Purchase Intention	65.67%	0.804***
Privacy Policy	69.63%	0.818***
Note: * denotes p<0.05, ** denotes p<0.01, *** denotes p<0.001		

Chapter 4 Findings and Discussion

4.1 Descriptive Statistical Analysis

4.1.1 Descriptive Statistical Analysis of Sample

With the help of SPSS, descriptive statistical analysis was conducted on the basic information of multiple individual variables in the study, including gender, age, educational background, consumption level, and occupation, as shown in Table 4.1 below.

Table 4.1 Descriptive Statistics of Sample

Variable	Category	Frequency	Percentage (%)
Gender	Male	188	48.2
	Female	202	51.8
Age	Under 18	56	14.4
	18–25 years old	139	35.6
	26–30 years old	95	24.4
	Over 30 years old	100	25.6
Educational Background	Junior high school	72	18.5
	High school	83	21.3
	College	82	21.0
	Bachelor's degree and above	153	39.2
Personal Consumption Level	Below 1000 yuan	67	17.2
	1000–2000 yuan	112	28.7
	2000–3000 yuan	71	18.2
	3000–5000 yuan	86	22.1
	Over 5000 yuan	54	13.8
Occupation	Student	142	36.4
	Public institution staff (including teachers) and government employees	35	9.0
	Self-employed	87	22.3
	Corporate employees	45	11.5
	Others	81	20.8

As shown in Table 4.1, males account for 48.2% and females for 51.8%, indicating a nearly 1:1 gender ratio. In terms of age, the group aged 18–25 makes up the largest proportion at 35.6%, highlighting the younger nature of e-commerce users. Regarding education, 39.2% of respondents hold a bachelor's degree or above, indicating good quality among the sample group. Additionally, students still comprise the majority, accounting for 36.4%. These results suggest that the data is well-distributed and representative of a wide range of e-commerce consumers.

4.1.2 Descriptive Statistics of Variables

Using SPSS, the mean, standard deviation, skewness, and kurtosis of each questionnaire item were calculated to analyze the distribution and check for normality. As shown in Table 4.2, the skewness and kurtosis values for all items are less than 2, indicating that the data follows a roughly normal distribution.

Table 4.2 Descriptive Statistics of Questionnaire Items

Variable		Item	Mean	Std.	Skewness		Kurtosis	
					Statistic	Std. Error	Statistic	Std. Error
Privacy Concern	Collection	1	3.93	1.225	-1.051	0.124	0.152	0.247
		2	3.94	1.126	-0.970	0.124	0.205	0.247
		3	4.01	1.166	-1.139	0.124	0.515	0.247
		4	4.01	1.190	-1.175	0.124	0.477	0.247
	Errors	5	4.01	0.990	-1.002	0.124	0.777	0.247
		6	4.09	0.971	-0.886	0.124	0.164	0.247
		7	4.10	0.913	-1.009	0.124	1.008	0.247
		8	4.10	0.932	-0.914	0.124	0.361	0.247
	Improper Access	9	4.17	0.942	-1.198	0.124	1.224	0.247
		10	4.13	0.886	-1.011	0.124	0.892	0.247
		11	4.17	0.899	-1.098	0.124	1.170	0.247
	Secondary Use	12	4.23	0.949	-1.318	0.124	1.524	0.247
		13	4.21	0.926	-1.258	0.124	1.557	0.247
		14	4.23	0.897	-1.261	0.124	1.790	0.247
		15	4.27	0.909	-1.349	0.124	1.784	0.247
Perceived Risk		16	4.08	0.885	-0.984	0.124	1.097	0.247
		17	3.96	0.941	-0.723	0.124	0.274	0.247
		18	4.01	0.914	-0.726	0.124	0.147	0.247
		19	4.12	0.938	-1.100	0.124	1.115	0.247
Purchase Intention		20	2.33	0.917	0.444	0.124	0.083	0.247
		21	2.09	0.907	0.737	0.124	0.650	0.247
		22	2.19	0.935	0.543	0.124	-0.010	0.247

	23	2.05	0.850	0.660	0.124	0.607	0.247
Privacy Policy	24	3.68	1.041	-0.547	0.124	-0.153	0.247
	25	3.68	0.980	-0.503	0.124	0.071	0.247
	26	3.70	1.011	-0.465	0.124	-0.200	0.247
	27	3.82	0.959	-0.629	0.124	0.189	0.247

4.2 Confirmatory Factor Analysis

It is generally accepted that standardized factor loadings for all items should be greater than 0.6. The Average Variance Extracted (AVE) should exceed 0.5, and the Composite Reliability (CR) should exceed 0.8. These criteria indicate that the measurement model has good convergent validity.

4.2.1 Confirmatory Factor Analysis of Privacy Concern

As shown in Table 4.3, the standardized factor loadings for all items under privacy concern are greater than 0.6. In this study, the four dimensions of privacy concern yield the following Composite Reliability (CR) values: 0.843, 0.821, 0.803, and 0.815, all of which exceed the standard of 0.8. The Average Variance Extracted (AVE) values are 0.574, 0.534, 0.576, and 0.525 respectively, all exceeding the threshold of 0.500. Thus, the scale shows good convergent validity.

Table 4.3 Validity Test for Privacy Concern Measurement Model

Variable		Item	Std. Factor Loading	CR	AVE
Privacy Concern	Collection	1	0.676	0.843	0.574
		2	0.826		
		3	0.746		
		4	0.774		
	Errors	5	0.742	0.821	0.534
		6	0.748		
		7	0.735		
		8	0.697		
	Improper Access	9	0.764	0.803	0.576
		10	0.751		
		11	0.762		
	Secondary Use	12	0.684	0.815	0.525
		13	0.801		
		14	0.687		
		15	0.720		

4.2.2 Confirmatory Factor Analysis of Perceived Risk

As shown in Table 4.4, all items under the perceived risk construct have standardized factor loadings above 0.6. The Composite Reliability (CR) of the perceived risk variable is 0.835, exceeding the standard threshold of 0.7. The AVE is 0.560, higher than the critical value of 0.500, indicating good convergent validity.

Table 4.4 Validity Test for Perceived Risk Measurement Model

Variable	Item	Std. Factor Loading	CR	AVE
Perceived Risk	16	0.759	0.835	0.560
	17	0.775		
	18	0.706		
	19	0.751		

4.2.3 Confirmatory Factor Analysis of Purchase Intention

As shown in Table 4.5, the standardized factor loadings of all items under purchase intention are above 0.6. The Composite Reliability (CR) is 0.825, meeting the 0.7 threshold. The AVE is 0.542, above the minimum requirement of 0.500. Therefore, the scale shows good convergent validity.

Table 4.5 Validity Test for Purchase Intention Measurement Model

Variable	Item	Std. Factor Loading	CR	AVE
Perceived Risk	20	0.731	0.825	0.542
	21	0.782		
	22	0.722		
	23	0.708		

4.2.4 Confirmatory Factor Analysis of Privacy Policy

As shown in Table 4.6, all items under the privacy policy construct have standardized factor loadings above 0.6. The Composite Reliability (CR) is 0.855, exceeding the 0.7 benchmark. The AVE is 0.595, higher than the minimum threshold of 0.500. Therefore, this scale also has good convergent validity.

Table 4.6 Validity Test for Privacy Policy Measurement Model

Variable	Item	Std. Factor Loading	CR	AVE
Perceived Risk	24	0.744	0.855	0.595
	25	0.794		
	26	0.759		
	27	0.788		

4.3 Structural Equation Model Testing

This study's research model focuses on the interrelationships among the four subdimensions of privacy concern, perceived risk, and users' purchase intention. AMOS was used to evaluate the model fit and verify its suitability. The maximum likelihood estimation method was applied. AMOS software was used to test the model fit. The fit indices and results are presented in Table 4.7. All model indicators met recommended thresholds, indicating good model fit and supporting the hypotheses proposed in this study.

Table 4.7 Model Fit Indices

Index Name	PCMIN/DF	RMSEA	GFI	IFI	NNFI	CFI
Model Value	1.771	0.045	0.919	0.958	0.951	0.958
Reference	< 3	< 0.1	> 0.9	> 0.9	> 0.9	> 0.9

4.4 Correlation Analysis

Using SPSS, a correlation analysis was conducted on the variables. As shown in Table 4.8, initial findings indicate that privacy concern (and its subdimensions), perceived risk, and purchase intention are significantly correlated. Each subdimension of privacy concern is positively related to perceived risk and negatively related to purchase intention. All correlation coefficients are below 0.7, suggesting no serious multicollinearity issues, thus supporting further regression and hypothesis testing.

Table 4.8 Correlation Matrix

Variable	Collection	Errors	Improper Access	Secondary Use	Perceived Risk	Privacy Policy	Purchase Intention
Collection	0.757						
Errors	0.410**	0.731					
Improper Access	0.370**	0.513**	0.759				
Secondary Use	0.251**	0.564**	0.575**	0.725			
Perceived Risk	0.330**	0.437**	0.393**	0.428**	0.748		
Privacy Policy	0.185**	0.335**	0.238**	0.274**	0.232**	0.736	
Purchase Intention	-0.340**	-0.490**	-0.426**	-0.418**	-0.387**	-0.666**	0.771
Note: * < 0.05, ** < 0.01, two-tailed test.							

4.5 Hypothesis Testing

To examine the direct relationships among privacy concern, perceived risk, and users' purchase intention, hierarchical regression analysis was conducted using SPSS. The analysis focused on three main pathways: (1) the impact of privacy concern on perceived risk, (2) the direct impact of privacy concern on purchase intention, and (3) the effect of perceived risk on purchase intention.

First, the results showed that all four subdimensions of privacy concern—collection, errors, Improper Access, and secondary use—had significant positive effects on perceived risk. Specifically, collection ($\beta = 0.277$, $p < 0.001$), errors ($\beta = 0.429$, $p < 0.001$), Improper Access ($\beta = 0.381$, $p < 0.001$), and secondary use ($\beta = 0.437$, $p < 0.001$) were all positively associated with consumers' perception of privacy-related risks. These results indicate that higher concern in each subdimension leads to increased perceived risk. Therefore, hypotheses H1a, H1b, H1c, and H1d are supported.

Second, all four dimensions of privacy concern demonstrated significant negative direct effects on purchase intention. The standardized coefficients show that collection ($\beta = -0.259$, $p < 0.001$), errors ($\beta = -0.466$, $p < 0.001$), Improper Access ($\beta = -0.415$, $p < 0.001$), and secondary use ($\beta = -0.439$, $p < 0.001$) negatively influence users' willingness to make purchases. These findings suggest that when consumers perceive higher privacy risks in these dimensions, their likelihood of purchasing decreases. Hence, hypotheses H3a, H3b, H3c, and H3d are also supported.

Lastly, the impact of perceived risk on purchase intention was assessed. The analysis revealed a significant negative relationship ($\beta = -0.382$, $p < 0.001$), indicating that the more consumers perceive privacy-related risk, the less likely they are to proceed with a purchase. This provides strong evidence in support of hypothesis H2.

In conclusion, the direct effect testing confirms that privacy concern significantly increases perceived risk and reduces purchase intention. Meanwhile, perceived risk also negatively influences purchase intention, suggesting its crucial role in mediating consumer decision-making processes in the context of privacy-sensitive environments.

Table 4.9 Direct Effect Test Results

Variable		Perceived Risk					Purchase Intention					
		M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11
Control Vari	Age	0.009	0.061	0.036	0.003	-0.004	0.079	0.030	0.049	0.086	0.093*	0.083*
	Education	0.054	0.053	0.043	0.028	0.007	0.026	0.027	0.038	0.054	0.073*	0.046

ables	Occupation	0.029	0.035	-0.001	0.029	0.025	-0.003	-0.036	0.003	-0.003	-0.025	-0.019
Independent Variables	Collection		0.277***					-0.259***				
	Errors			0.429***					-0.466***			
	Improper Access				0.381***					-0.415***		
	Secondary Use					0.437***					-0.439***	
Mediator Variable	Perceived Risk											-0.382***
F		0.008	0.129	0.197	0.159	0.186	0.011	0.123	0.248	0.200	0.201	0.165
R²		0.001	0.120	0.189	0.150	0.177	0.003	0.114	0.240	0.192	0.193	0.157
Adjusted R²		1.082	14.270***	23.690***	18.130***	21.930***	1.441	13.510***	31.710***	24.130***	24.280***	19.070***
Note: * p< 0.05, ** p< 0.01, *** p< 0.001, two-tailed test.												

4.6 Mediation Effect Analysis

To examine whether perceived risk mediates the relationship between privacy concern and users' purchase intention, a series of regression analyses were conducted. First, four models (M12–M15) were established, with perceived risk as the mediator variable. Compared to the direct effect models (M7–M10), the inclusion of perceived risk led to a noticeable decrease in the absolute value of regression coefficients for all four privacy concern subdimensions—collection, errors, improper access, and secondary use—when predicting purchase intention. Specifically, the coefficients for the paths from collection (β = -0.174, $p < 0.001$), errors (β = -0.373, $p < 0.001$), improper access (β = -0.317, p < 0.001), and secondary use (β = -0.331, p < 0.001) to purchase intention were significantly reduced after including perceived risk, indicating that perceived risk partially mediates these relationships.

To further confirm the mediating role of perceived risk, a Bootstrap method was employed using the SPSS PROCESS macro. The mediation effect was tested under a 95% confidence interval. The results showed that the indirect effects of all four dimensions were significant, and their confidence intervals did not include zero. Specifically, for collection, the indirect effect was -0.077 (95% CI: [-0.127, -0.039]); for errors, -0.089 (95% CI: [-0.162, -0.034]); for improper access, -0.097 (95% CI: [-0.165, -0.045]); and for secondary use, -0.108 (95% CI: [-0.181, -0.052]). These results provide strong evidence that perceived risk plays a significant mediating role in the influence of privacy concern on purchase intention.

In summary, both the hierarchical regression and bootstrap analysis confirm that perceived risk acts as a partial mediator in the relationship between each privacy concern subdimension and purchase intention. Therefore, hypotheses H4a, H4b, H4c, and H4d are supported.

Table 4.10 Mediation Effect Test Results

Variable		Purchase Intention			
		M12	M13	M14	M15
Control Variables	Age	0.049	0.057	0.087*	0.092*
	Education	0.430	0.047	0.061*	0.075*
	Occupation	-0.025	0.003	-0.023	-0.019
Independent Variables	Collection	-0.174***			
	Errors		-0.373***		
	Improper Access			-0.317***	
	Secondary Use				-0.331***
Mediator Variable	Perceived Risk	-0.306***	-0.217***	-0.256***	-0.247***
F		0.210	0.288	0.259	0.254
R^2		0.200	0.279	0.250	0.245
Adjusted R^2		20.390***	31.060***	26.880***	26.180***
Note: * p< 0.05, ** p< 0.01, *** p< 0.001, two-tailed test.					

Table 4.11 Mediation Analysis

Pathway	Coefficient	Std. Error	T	P	LLCT	CLCI
Collection →Purchase Intention	-0.256	0.044	-5.875	0.000	-0.342	-0.171

Collection → Perceived Risk	-0.180	0.042	-4.262	0.000	-0.263	-0.097
Collection → Perceived Risk → Purchase Intention	-0.077	0.022		0.000	-0.127	-0.039
Errors →Purchase Intention	-0.466	0.051	-9.186	0.000	-0.565	-0.366
Errors → Perceived Risk	-0.377	0.060	-6.301	0.000	-0.494	-0.259
Errors → Perceived Risk → Purchase Intention	-0.089	0.033		0.000	-0.162	-0.034
Improper Access →Purchase Intention	-0.404	0.046	-8.863	0.000	-0.493	-0.341
Improper Access → Perceived Risk	-0.307	0.049	-6.294	0.000	-0.403	-0.211
Improper Access → Perceived Risk → Purchase Intention	-0.097	0.030		0.000	-0.165	-0.045
Secondary Use →Purchase Intention	-0.415	0.055	-7.610	0.000	-0.522	-0.308
Secondary Use → Perceived Risk	-0.307	0.058	-5.335	0.000	-0.420	-0.194
Secondary Use → Perceived Risk → Purchase Intention	-0.108	0.033		0.000	-0.181	-0.052

4.7 Moderation Effect Analysis

To test the moderating effect of privacy policy on the relationship between privacy concern and perceived risk, the raw data were first standardized (mean = 0, standard deviation = 1). Hierarchical regression analysis was then conducted to examine interaction effects. By observing the changes in R^2 and F values, as well as the significance of interaction terms, moderation effects can be determined. If the adjusted R^2 increases substantially and the interaction term is significant, it indicates the presence of a moderating effect.

As shown in Table 4.12, M16 is the regression model of the collection dimension of privacy concern predicting perceived risk, and M17 includes the interaction term between collection and privacy policy. The result shows that the interaction term is not significant and the R^2 change is minimal, indicating that privacy policy does not moderate the relationship between collection and perceived risk. Thus, hypothesis H5a is not supported.

M18 is the model for the error dimension predicting perceived risk, and M19 includes the interaction between errors and privacy policy. Again, the interaction term is not significant and R^2 change is small, suggesting that privacy policy does not moderate the relationship between errors and perceived risk. Therefore, hypothesis H5b is not supported.

M20 is the model of improper access predicting perceived risk, and M21 includes the interaction between improper access and privacy policy. The main effect is significant ($\beta = 0.307$, $p < 0.001$), and the interaction term is also significant ($\beta = -0.157$, $p < 0.01$), indicating that privacy policy moderates the relationship between improper access and perceived risk. Thus, hypothesis H5c is supported.

M22 is the model of secondary use predicting perceived risk, and M23 includes the interaction between secondary use and privacy policy. Results show the main effect is significant ($\beta = 0.329$, $p < 0.001$) and the interaction term is also significant ($\beta = -0.135$, $p < 0.01$), indicating that privacy policy moderates the relationship between secondary use and perceived risk. Therefore, hypothesis H5d is supported.

It is worth noting that the main variables (improper access and secondary use) positively predict perceived risk, while the interaction terms with privacy policy are negative. This implies a negative moderating effect, where privacy policy weakens the impact of these privacy concerns on perceived risk.

Table 4.12 Moderation Effect Test of Privacy Policy

Variable		Perceived Risk							
		M16	M17	M18	M19	M20	M21	M22	M23
Control Variables	Age	0.064	0.064	0.039	0.040	0.010	0.003	0.003	0.004
	Education	0.080*	0.078*	0.060	0.063	0.053	0.043	0.030	0.019
	Occupation	0.033	0.034	0.001	0.000*	0.028	0.033	0.024	0.027
Main Effect	Collection	0.248***	0.244***						

	Errors			0.389***	0.404***				
	Improper Access					0.338***	0.307***		
	Secondary Use							0.393***	0.329***
	Privacy Policy	0.180***	0.181***	0.109*	0.108*	0.149***	0.153***	0.121**	0.124**
Interaction Term	Collection ×Privacy Policy		-0.022						
	Errors ×Privacy Policy				0.033				
	Improper Access ×Privacy Policy						-0.157**		
	Secondary Use ×Privacy Policy								-0.135*
F		15.217***	12.706***	20.370***	17.042***	17.152***	15.918***	19.319***	17.304***
R^2		0.165	0.166	0.210	0.211	0.183	0.200	0.201	0.213
Adjusted R^2		0.155	0.153	0.199	0.198	0.172	0.187	0.191	0.201
Note: $^*p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$ (two-tailed test)									

Table 4.13 Hypothesis Test Results

Hypothesis	Items	Result
H1	Privacy concern has a positive impact on perceived risk.	supported
H1a	Collection has a positive impact on perceived risk.	supported
H1b	Errors have a positive impact on perceived risk.	supported
H1c	Improper access has a positive impact on perceived risk.	supported
H1d	Secondary use has a positive impact on perceived risk.	supported
H2	Perceived risk has a negative impact on purchase intention.	supported

H3	Privacy concern has a negative impact on purchase intention.	supported
H3a	Collection has a negative impact on purchase intention.	supported
H3b	Errors have a negative impact on purchase intention.	supported
H3c	Improper access has a negative impact on purchase intention.	supported
H3d	Secondary use has a negative impact on purchase intention.	supported
H4	Perceived risk mediates the relationship between privacy concern and purchase intention.	supported
H4a	Perceived risk mediates the relationship between collection and purchase intention.	supported
H4b	Perceived risk mediates the relationship between errors and purchase intention.	supported
H4c	Perceived risk mediates the relationship between improper access and purchase intention.	supported
H4d	Perceived risk mediates the relationship between secondary use and purchase intention.	supported
H5	Privacy policy moderates the relationship between privacy concern and perceived risk.	supported
H5a	Privacy policy moderates the relationship between collection and perceived risk.	supported
H5b	Privacy policy moderates the relationship between errors and perceived risk.	supported
H5c	Privacy policy moderates the relationship between improper access and perceived risk.	supported
H5d	Privacy policy moderates the relationship between secondary use and perceived risk.	supported

4.8 Discussion

The results show that privacy concern has a significant positive effect on perceived risk; that is, the higher the degree of privacy concern, the stronger the user's perception of risk. From a theoretical perspective, e-commerce transactions between platforms and users are often based on some form of contractual relationship, which maintains a balance in information exchange. Once this balance is disrupted, users tend to become more alert and pay closer attention to how their personal information is used, which intensifies their perception of risk. Consequently, users may adopt a series of protective measures to safeguard their privacy information.

However, users with a high level of privacy concern are often already alert and have taken preventive actions before any such disruption occurs. They are cautious from the start and generally distrust e-commerce platforms that do not provide sufficient guarantees for personal information protection. Therefore, these users typically perceive higher risk than others.

The findings indicate that perceived risk has a significant negative effect on purchase intention. When users perceive risk during their interactions with e-commerce platforms—such as the possibility of information misuse or inadequate privacy protection—they are more likely to reduce or even stop their purchasing behavior. Users may continue using platforms cautiously only if they feel their privacy is well protected. Otherwise, the emergence of perceived risk could lead to negative emotions and avoidance behavior, including suspending purchases or abandoning shopping carts. In essence, perceived risk acts as a psychological barrier that suppresses purchasing intention.

The results also reveal that privacy concern has a significant negative effect on purchase intention. When users interact with a particular e-commerce platform, if they perceive that the platform frequently collects personal data without clear consent or uses the data in ways that violate user expectations, their trust in the platform declines. Users may feel that their privacy is at risk and may choose to reduce engagement or stop using the platform altogether.

In practice, when users are required to register on a platform or activate features linked to sensitive data, they may assess the platform as unsafe. In such cases, users may avoid the platform, stop using it, or warn their peers against it. This reflects the negative impact of privacy concern on consumers' willingness to purchase.

The results show that perceived risk plays a mediating role in the relationship between privacy concern and purchase intention. In other words, in the context of e-commerce, the degree of perceived risk partially explains how privacy concern affects users' willingness to purchase. For instance, when users are required to fill in personal details on a platform, they may worry about how this information will be stored, used, or leaked, which further triggers perceived risk and influences their decision to buy.

This study confirms the chain mechanism where privacy concern increases perceived risk, which in turn reduces purchase intention. For e-commerce platforms, it is crucial to reduce perceived risk by strengthening privacy protection policies and implementing secure practices. This can help lower the barrier caused by privacy concern, encouraging users to proceed with purchases and boosting economic activity.

The empirical results indicate that privacy policy partially moderates the relationship between privacy concern and perceived risk. Specifically, regression analysis revealed that privacy policy has a significant negative moderating effect, meaning that effective privacy policies can mitigate the degree to which privacy concern increases perceived risk.

The moderation effect is particularly significant in the cases of improper access and secondary use. That is, privacy policies can buffer users' perceived risk when they are concerned about these two dimensions. However, the moderation effects are not significant in the collection and errors dimensions, indicating that privacy policy does not consistently alleviate perceived risk across all areas of privacy concern.

In practice, most e-commerce platforms now offer online privacy policies, but due to vague definitions and poor standardization, users may find the content unclear or unconvincing. Without clear guidance, users cannot effectively assess whether their privacy is protected. Often, privacy policies serve only as a symbolic function for the platform rather than offering substantive protection. Moreover, legal enforcement is weak, and platforms are not held accountable for non-compliance.

Additionally, users often lack alternative options to accept or reject privacy terms, which results in weak practical protection. Many users believe that even after agreeing to a privacy policy, their information might still be misused. In short, privacy policy does not significantly mitigate the effects of privacy concern on perceived risk unless the policy is clearly defined, well enforced, and user-centered.

Chapter 5 Conclusion and Recommendation

5.1 Conclusion

1. Privacy concern has a significant negative effect on purchase intention. In the era of big data, personal information is critical for the development of e-commerce platforms. While the use of data enables diversified marketing strategies and business models, if platforms neglect the protection of personal information, users may lose trust and refrain from purchasing. Therefore, reducing user privacy concerns and enhancing platform credibility is key to improving purchase intention and driving platform profitability.

2. Privacy concern has a significant positive effect on perceived risk. In an e-commerce context, perceived risk remains a crucial factor influencing consumer behavior. When e-commerce platforms fail to provide sufficient safeguards for personal data, users become more aware of potential misuse. The more concerned users are, the more they will question the platform's capacity to securely manage their data, which in turn increases their perceived risk.

3. Perceived risk has a significant negative effect on purchase intention. Users weigh the trade-off between data disclosure and potential benefits. If the risks outweigh the benefits, users are more likely to avoid using the platform. When users perceive a platform as unsafe, they are likely to withhold transactions or switch to alternative services. Therefore, risk perception is a psychological barrier to actual purchasing behavior.

4. Perceived risk mediates the relationship between privacy concern and purchase intention. In e-commerce environments, large volumes of data storage and personal information collection often lack transparent consent. This heightens perceived risk, which reduces users' willingness to buy. In other words, perceived risk is the psychological pathway through which privacy concern translates into lower purchase intention.

5. Privacy policy plays a partial moderating role in the relationship between privacy concern and perceived risk. The more users trust the effectiveness of a privacy policy, the less intensely they perceive privacy risk. Therefore, well-designed policies can regulate users' perceptions and reduce privacy-related anxiety. E-commerce companies should establish effective privacy policies and ensure their actual enforcement to improve data security, increase user trust, and ultimately drive transaction behavior.

5.2 Recommendation

The most effective way to protect personal information is to prevent privacy issues at the source. This requires enhancing users' awareness of personal privacy protection. In today's digital environment, users must have the ability to identify potential privacy risks and avoid unknowingly providing personal information that may be collected and misused. Users should not easily share personal data on unfamiliar websites or scan unknown QR codes, and they should develop the habit of refusing requests for irrelevant data collection. Users must understand their rights and obligations in protecting their data, and actively build a secure and healthy digital environment.

E-commerce platforms must prioritize legal compliance and promptly address any violations. They should set up reporting mechanisms so users can quickly flag issues and receive feedback. Privacy policies should be clearly written and easy to understand. They must outline data collection practices and the platform's obligations. A unified privacy policy format should be adopted across platforms for easier management and supervision. Additionally, platforms should improve their brand image by enhancing product and service quality and providing more personalized recommendations to increase user loyalty and economic value.

Governments play a vital role in privacy protection by formulating adaptable laws that address evolving privacy threats in e-commerce. Laws should regulate how personal data is collected, stored, and shared, and require platforms to disclose how user data is handled. Government agencies should monitor enforcement, issue penalties for violations, and publish blacklists to deter illegal behavior. The government should also support non-profit privacy organizations, train personnel, and ensure that privacy protection remains a key aspect of digital governance.

5.3 Further Study

Future studies should expand beyond a single demographic or geographic group. Including diverse age groups, income levels, and cultural backgrounds would enhance the generalizability of the findings and uncover potential moderating variables such as digital literacy or regional privacy regulations. And to examine how evolving privacy policies or data breaches affect users' privacy concern, risk perception, and purchase behavior over time.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Bagozzi, R. P. (1989). An investigation into the role of intentions as mediators of the attitude-behavior relationship. *Journal of Economic Psychology, 10*(1), 35–62.

Bansal, G., & Zahedi, F. (2008). Efficacy of privacy assurance mechanisms in the context of disclosing health information online. *AMCIS 2008 Proceedings, (178)*, 1–11.

Bauer, R. A. (1960). Consumer behavior as risk taking. In R. S. Hancock (Ed.), *Dynamic marketing for a changing world* (pp. 389–398). Proceedings of the 43rd Conference of the American Marketing Association.

Berry, L. L., & Parasuraman, A. (1996). The behavioral consequences of service quality. *Journal of Marketing, 60*(2), 31–46.

Bettman, J. R. (1973). Perceived risk and its components: A model and empirical test. *Journal of Marketing Research, 10*(2), 184–190.

Castaneda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research, 7*(2), 117–141.

Chaiken, S. R. (1991). Comprehension's role in persuasion: The case of its moderating effect on the persuasive impact of source cues. *Journal of Consumer Research, 18*(1), 52–62.

Chen, Y., Li, T., & Wang, H. (2020). Data privacy breaches in e-commerce: Causes and consequences. *Journal of Cybersecurity, 8*(2), 145–160.

CNNIC. (2024). *The 53rd statistical report on China's internet development*. China Internet Network Information Center. https://www.cnnic.net.cn/

Cox, D. F., & Rich, S. U. (1964). Perceived risk and consumer decision-making—The case of telephone shopping. *Journal of Marketing Research, 1*(4), 32–39.

Cui, J. (2019). The impact of perceived risk on consumers' online impulse buying. *Social Science Front, (4)*, 254–258.

Dong, D. (2007). Research on the sources, types, and influencing factors of online shopping risks. *Journal of Dalian University of Technology (Social Science Edition), 28*(2), 13–19.

Dodd, S. R., William, B., Monroe, K. B., et al. (1991). The effect of price, brand, and store information on buyers' product evaluation. *Journal of Marketing Research, 28*(3), 307–319.

Du, W., Fang, L., & Chen, L. (2023). Differences in factors influencing purchase intention between traditional e-commerce and content platform live-streaming for clothing. *Economic Research Guide, (5)*, 85–87.

Fasolo, B., McClelland, G. H., & Lange, K. A. (2005). The effect of site design and interattribute correlations on interactive web-based decisions. *Journal of Behavioral Decision Making, 18*(1), 1–22.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Addison-Wesley.

Gao, C., & Xie, Y. (2023). The impact of corporate privacy policies and their mechanisms: A review and outlook from the user perspective. *Journal of Capital University of Economics and Business, 25*(5), 95–112.

Gao, Z. (2022). Research on online purchase intention of fresh agricultural products based on perceived risk and perceived benefit. *Jiangnan University*.

Gong, X., Zhang, Z. K., Chen, C., et al. (2019). What drives self-disclosure in mobile payment applications? The effect of privacy assurance approaches, network externality, and technology complementarity. *Information Technology & People, 33*(4), 1174–1213.

Guo, Y., Wang, X., & Wang, C. (2021). Impact of privacy policy content on perceived effectiveness of privacy policy: The role of vulnerability, benevolence, and privacy concern. *Journal of Enterprise Information Management, 35*(3), 774–795.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275–298.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management, 1*(1–2), 45–71.

Kahneman, D., & Tversky, A. (2008). Prospect theory: An analysis of decision under risk. *Economic Information Review, (1)*, 1–18.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564.

Kim, S., & Park, J. (2022). Consumer risk perception and mitigation strategies in online shopping. *International Journal of Electronic Commerce, 26*(1), 78–95.

Lee, M., Brown, A., & Davis, R. (2021). Big data and personalized marketing in e-commerce. *Journal of Retailing, 97*(3), 412–428.

Li, J., Yan, X., Zhang, J., & Zhou, Y. (2023). Research on the influence mechanism of privacy disclosure behavior among young WeChat users: The mediating effect of privacy cynicism. *Journal of Journalism and Communication Review, 76*(1), 87–101.

Li, R., Gao, X., & Bi, W. (2023). Research on the influence mechanism of consumers' online purchase intention in store live-streaming. *Journal of Harbin University of Commerce (Social Science Edition), (6)*, 87–96.

Li, X. (2021). Research on college students' mobile phone dependence behavior from the perspective of planned behavior theory. *Dalian University of Technology*.

Liu, X., Zhang, W., & Zhao, Y. (2023). Digital inclusion among elderly internet users in China. *Computers in Human Behavior, 139*, 107521.

Liu, Y., & Wei, Y. (2022). Analysis of research hotspots and trends in the theory of planned behavior. *Cooperative Economy and Technology, (3)*, 107–109.

Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison. *Information & Management, 55*(8), 1005–1023.

Lu, B., Fan, W., & Zhou, M. (2016). Social presence, trust, and social commerce purchase intention: An empirical study. *Computers in Human Behavior, 56*, 225–237.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 335–361.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2–17.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62–73.

Shi, H. (2023). The impact of perceived risk on consumers' behavioral intentions on cross-border e-commerce platforms. *Journal of Dalian Maritime University (Social Science Edition), 22*(5), 63–73.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.

Smith, J., & Johnson, K. (2022). The evolution of e-commerce: Trends and future directions. *E-Commerce Research, 15*(4), 301–317.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36–47.

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

Tan, J., Lyu, X., & Han, X. (2023). Research on the influence mechanism of individual privacy protection behavior based on the "attitude-intention-behavior" framework. *Information Science, (1)*, 8–15.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1–22.

Wang, D., & Wang, G. (2013). Perceived risk of consumers' online shopping under information asymmetry. *Economic Management, 35*(1), 142–152.

Wang, E. S. T. (2019). Effects of brand awareness and social norms on user-perceived cyber privacy risk. *International Journal of Electronic Commerce, 23*(2), 272–293.

Wang, L., & Zhang, Q. (2023). Ethical issues in consumer data collection: A global perspective. *Business Ethics Quarterly, 33*(1), 89–110.

Wang, W., & Song, T. (2023). Research on the mechanism and optimization of intermittent discontinuation behavior among short video users. *Modern Information, 43*(12), 51–62.

Wang, Y. (2020). On the effectiveness of online privacy policies: Focusing on personal information protection. *Comparative Law Research, (1)*, 120–134.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166–170.

Xue, R., Wang, P., & Yao, B. (2022). The impact of WeChat marketing by clothing companies on college students' purchase intention. *China Management Informationization, 25*(15), 107–111.

Ye, L. (2023). Research on the influencing factors of farmers' participation in agricultural product e-commerce: Based on micro-survey data from farmers in Gansu. *Journal of Commercial Economics, (21)*, 108–112.

Yuan, X., & Niu, J. (2021). An empirical study on social media privacy policies and user self-disclosure: A moderated mediation model. *Journal of Information Resources Management, 11*(1), 49–58.

Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: A means-end model and synthesis of evidence. *Journal of Marketing, 52*(3), 2–22.

Zhou, F., & Li, N. (2021). Privacy concerns and online purchase behavior: The mediating role of perceived risk. *Journal of Consumer Behaviour, 40*(5), 612–625.

Appendix

Survey on the Impact of Privacy Concern on Users' Purchase Intention

Part 1: Introduction

Dear Sir/Madam,

Hello! This is an academic research survey. Thank you for taking the time to participate. This questionnaire aims to explore your level of concern about the collection and continued use of personal information on e-commerce platforms. The survey is anonymous, and the results will be used strictly for academic research. All information you provide will be kept strictly confidential. Please read the questions carefully and answer them based on your actual experience.

Thank you once again for your support and assistance! We wish you success in your work and happiness in life!

Part 2: Basic Information

1. Your Gender

A. Male B. Female

2. Your Age

A. Under 18 B. 18–25 C. 26–30 D. Over 30

3. Your Education Level

A. Junior High School B. High School/Vocational School C. Associate Degree D. Bachelor's Degree or Above

4. Your Monthly Personal Expenditure

A. Below 1,000 RMB B. 1,000–2,000 RMB C. 2,000–3,000 RMB D. 3,000–5,000 RMB E. Above 5,000 RMB

5. Your Occupation

A. Student

B. Public Sector Employee (including teachers) and Government Personnel

C. Self-employed

D. Corporate Employee

E. Other

Part 3: Privacy Concern

Please read the following statements related to your concern about personal information when making purchases on e-commerce platforms. Based on your actual feelings, select the most appropriate number to indicate your level of agreement:

1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

Collection

1. I feel quite disturbed when an e-commerce website asks permission to collect my personal information.

2. When an e-commerce website asks to collect my personal data, I need to think carefully.

3. Providing personal data to different e-commerce websites makes me feel uneasy.

4. I mind it when e-commerce websites collect too much of my personal data.

Errors

1. I doubt the accuracy of the information retained by the e-commerce website.

2. I worry about possible errors in the personal data processing by the e-commerce website.

3. I worry that the accuracy of personal information may decrease due to excessive data volume.

4. I believe personal data stored by the website should be double-checked for accuracy.

Improper Access

1. I worry that my personal data may be accessed by Improper external parties.

2. I believe e-commerce websites should seek my permission before accessing my data.

3. I worry that personal data stored on e-commerce platforms might be accessed without permission.

Secondary Use

1. I suspect that e-commerce platforms might sell personal data to third-party companies.

2. I worry that e-commerce platforms may use personal data for purposes not explicitly stated.

3. I worry that e-commerce platforms may share users' personal information with others.

4. I mind it when my personal information is used by people or entities unknown to me.

Part 4: Perceived Risk

Please read the following statements related to the risks you perceive when providing personal information on e-commerce platforms. Select the number that best reflects your actual feelings:

1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

1. I believe there is a certain risk in providing personal data to e-commerce platforms.

2. I believe personal data disclosure on e-commerce platforms may result in certain losses.

3. I believe sharing personal data with e-commerce platforms may cause concerns or problems.

4. I believe providing personal data to e-commerce platforms results in significant uncertainty.

Part 5: Purchase Intention

Please read the following statements related to your purchase intentions on e-commerce platforms and select the number that best reflects your actual feelings:

1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

1. I would recommend this e-commerce platform to my friends.

2. I am willing to continue using this e-commerce platform.

3. Compared to offline shopping, I prefer to buy any product via this e-commerce platform.

4. If I need a product soon, I may consider purchasing it via this e-commerce platform.

Part 5: Purchase Intention

Please read the following items regarding your purchase behavior on e-commerce platforms. Select the number that best reflects your true feelings:

1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

1. I would recommend this e-commerce platform to my friends.

2. Overall, I am willing to continue using this e-commerce platform.

3. Compared to offline options, I prefer to purchase any needed products through this platform.

4. If I need something soon, I may consider purchasing it via this e-commerce platform.

Part 6: Privacy Policy

Please read the following items about your concerns regarding the privacy policy when shopping on e-commerce platforms. Select the number that best reflects your true feelings:

1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

1. I believe the e-commerce platform fulfills all the privacy policy promises it makes.

2. I believe the platform's privacy policy can guarantee the security of my personal information.

3. I believe the platform's privacy policy reduces my privacy concerns.

4. I believe the platform's privacy policy effectively protects my personal information.

บันทึกข้อความ

ส่วนงาน บัณฑิตวิทยาลัย สาขาบริหารธุรกิจ โทร.ภายใน 5336

ที่ มส 0210.01 / 0266 **วันที่** 14 กันยายน 2568

เรื่อง ขออนุมัติสำเร็จการศึกษาประจำปีการศึกษา 2567

เรียน ท่านอธิการบดี

__เรื่องเดิม__ นักศึกษาหลักสูตรบริหารธุรกิจมหาบัณฑิต MISS. WANG ZHEN รหัสนักศึกษา 6417195009 ได้ศึกษารายวิชาครบถ้วนสมบูรณ์ และได้ปฏิบัติตามเกณฑ์สำเร็จการศึกษาตามที่มหาวิทยาลัยสยามกำหนดเรียบร้อยแล้ว ทั้งนี้พร้อมยื่นเรื่องขออนุมัติสำเร็จการศึกษา โดยมีรายละเอียด ดังต่อไปนี้

1. ผ่านการตรวจสอบความซ้ำซ้อนด้วยโปรแกรม Grammarly เมื่อวันที่ 16 สิงหาคม 2568
2. ผ่านการสอบประมวลความรู้ข้อเขียน เมื่อวันที่ 26 เมษายน 2568
3. ผ่านการสอบปากเปล่าขั้นสุดท้ายวิชาการค้นคว้าอิสระ เมื่อวันที่ 8 พฤษภาคม 2568
4. ผ่านเกณฑ์มาตรฐานความรู้ภาษาอังกฤษ Oxford Placement Test score 100 CEFR C2 เมื่อวันที่ 15 มีนาคม 2568
5. ผ่านการประชุมวิชาการระดับนานาชาติ at The 18th National and International Academic Conference on "Sustainable Horizon: Transforming Ideas into Impact" Subject : A Case Study of the Influence of Privacy Concerns on Users' Purchase Intention in E-Commerce Environment on 6-7 August 2025, United Nations Conference Centre Bangkok Thailand

__เรื่องพิจารณา__ เพื่อพิจารณาเข้าประชุมสภามหาวิทยาลัย และอนุมับตินักศึกษาสำเร็จการศึกษา ประจำปีการศึกษา 2567 ดังรายละเอียดเอกสารประกอบการสำเร็จการศึกษาตามที่แนบมา

จึงเรียนมาเพื่อพิจารณาอนุมัติ และให้ดำเนินการต่อไป

(รศ.ดร.จอมพงศ์ มงคลวนิช)
คณบดีบัณฑิตวิทยาลัย สาขาบริหารธุรกิจ

ตรวจสอบหลักฐาน IS เรียบร้อยแล้ว

19 ก.ย.68