BILINGUAL PUBLISHING GROUP

Journal of Sustainable Business and Economics

https://journals.bilpubgroup.com/index.php/jsbe

RESEARCH ARTICLE

Research on Residents' Willingness to Protect Privacy in the Context of the Personal Information Protection Law: A Survey Based on Foshan Residents' Data

*Xiying Huang, Qizhao Xie, Xunxun Jiang, Zhihang Zhou, Xiao Zhang, Yiyuan Cheng, Yu'nan Wang, Chien Chi Chu**

School of Economics and Management, Foshan University, Guangdong, 528000, China

ABSTRACT

The Personal Information Protection Law, as the first law on personal information protection in China, hits the people's most concerned, realistic and direct privacy and information security issues, and plays an extremely important role in promoting the development of the digital economy, the legalization of socialism with Chinese characteristics and social public security, and marks a new historical development stage in the protection of personal information in China. However, the awareness of privacy protection and privacy protection behavior of the public in personal information privacy protection is weak. Based on the literature review and in-depth understanding of current legal regulations, this study integrates the relevant literature and theoretical knowledge of the Personal Protection Law to construct a conceptual model of "privacy information protection willingness—privacy information protection behavior". Taking the residents of Foshan City as an example, this paper conducts a questionnaire survey on their attitudes toward the Personal Protection Law, analyzes the factors influencing their willingness to protect their privacy and their behaviors, and explores the mechanisms of their influencing variables, to provide advice and suggestions for promoting the protection of privacy information and building a security barrier for the high-quality development of public information security.

Keywords: Personal Information Protection Law; Privacy security; Privacy protection will

*CORRESPONDING AUTHOR:
Chien Chi Chu, School of Economics and Management, Foshan University, Guangdong, 528000, China; Email: 1445730799@qq.com

ARTICLE INFO
Received: 12 July 2023 | Received in revised form: 9 August 2023 | Accepted: 11 August 2023 | Published: 18 August 2023
DOI: https://doi.org/10.30564/jsbe.v6i3.5840

CITATION
Huang, X.Y., Xie, Q.Zh., Jiang, X.X., et al., 2023. Research on Residents' Willingness to Protect Privacy in the Context of the Personal Information Protection Law: A Survey Based on Foshan Residents' Data. Journal of Sustainable Business and Economics. 6(3): 37-54. DOI: https://doi.org/10.30564/jsbe.v6i3.5840

1. Introduction

In the era of big data information, the theme of the Internet gradually extends from the technology itself to various fields of social economy and production life, and the circulation of personal information and the sharing of data among them undoubtedly make the data the foundation of the overall development of society. As a result, the commerciality of the value carried by personal information has gradually increased, and the conflict between the value of personal data information and the urgency of personal privacy protection has become a focus of social concern. However, in the face of the collection, storage and processing of Internet user data by super-enterprise platforms, the majority of users have no way of knowing who is using their personal information data. Although corporate platforms provide privacy policy statements, users are unable to protect their data through privacy policies due to the disparity in power between companies and users and the strong compulsory nature of privacy policies; in the face of increasingly personalized service functions and the pursuit of personal information sharing, more and more people choose to provide their personal data to Internet platforms or authorize them to Internet platforms to collect chat data, consumption data, browsing data, location data, etc. And in order to gain more business interests, companies tend to collect data information and analyze their personal behaviors and preferences by various means to gain insight into each user. This not only forms the leakage of personal information, but also comes with the problem of illegal use and trafficking of personal information. With the emergence of various social phenomena and the exposure of problems, users are concerned about the safety and protection of their privacy, and thus the degree of privacy concern is increasing with the times.

In August 2021, the State introduced the Personal Information Protection Law (hereinafter referred to as the "Personal Protection Law"), which aims to regulate the collection and use of personal privacy information by enterprises and prevent the misuse of information, etc. In order to maintain social security and safeguard people's privacy, the regulation also officially came into force on November 1, 2021. The Personal Protection Law, as the first law for personal information protection in China, responds to the most concerned and direct interests of the people, and makes adequate responses to the governance of the country and the concerns of the society. It further strengthens the legal protection of personal privacy information in China, builds a "protection net" and "safety net" for people's personal information security in the era of the Internet and big data, pries the balance board of interests and fairness through legal leverage, realizes the leap from privacy to data right protection, and promotes the social protection. It is a new milestone in the field of information protection in China, which is a leap from the right to privacy to the right to data protection and promotes the development of good social construction.

Based on this background, this paper conducts questionnaires and in-depth interviews with Foshan residents as well as in-depth data processing and analysis through field research and in-depth analysis of factors affecting the willingness to protect personal privacy information by constructing a numerical model to understand the residents' willingness to protect personal privacy information with the introduction of the Personal Protection Law, their attitudes towards the existing network information operation mode and their expectations for future development; to understand the residents' awareness of their In the Internet era, the awareness of personal privacy information security and the acceptance of precision marketing in the Internet and its scope. At the same time, this study breaks away from previous research ideas and analyzes various factors that affect residents' willingness to protect privacy, starting from the Personal Information Protection Law that will be officially implemented in November 2021 and the application to join the Digital Economy Partnership Agreement on October 30, 2021, in terms of "privacy concerns", "response effectiveness", "risk perception", "self-efficacy", and "privacy violation experience" as the basis, and introduces a new variable The new variable "knowledge of privacy" was introduced as an independent variable to investigate the factors influencing residents' willingness to protect privacy information. In this way, the study aims to provide an opportunity for residents to increase their willingness to protect personal privacy information, raise their awareness of privacy protection, and enhance their ability to protect privacy information; for platform companies to find a balance board between digital marketing and digital operation and user privacy in the market environment of the Personal Protection Law and other "new laws", and for the implementation of digital marketing reform in the new era, as well as the implementation of digital marketing reform in the Personal Protection Law and other privacy laws. Privacy Law and other privacy laws to provide theoretical support for enterprises and marketing services to change their thinking and strategies, for e-commerce, network platforms, etc. in the new legal environment to better balance their own interests and user privacy protection; for the government to regulate the Internet environment and promote the healthy and orderly development of e-commerce and network platforms to provide policy recommendations to further improve personal privacy protection law, improve the residents of the network personal privacy To further improve the personal privacy protection law, improve residents' awareness of online personal privacy protection, reduce the occurrence of online privacy infringement, maintain social public information security, promote the development of socialism with Chinese characteristics under the rule of law, so as to better promote the development of social public security, maintain social peace and harmony and stability, and promote the healthy and stable development of economy and society.

2. Literature review and research hypothesis

2.1 Literature review

Foreign research on personal information protection is earlier than that of China, and accordingly, personal information protection in the form of legislation is also earlier than that of China. For the study of personal information security protection measures, many foreign scholars adopt the research perspective of user and operator level to analyze the countermeasures of personal information security protection, Malandrino D and Scarano (2013) believe that in order to protect personal privacy and personal information security, users must further enhance the awareness of information protection [1]. Baruh L (2012) argues that the maturity of information technology in the era of big data has facilitated people's daily life, but it also further increases the risk of personal information security [2]. In the study of personal information security protection measures, scholars pay more attention to the behavior of users and merchants, and regulating merchants' information management behavior and enhancing users' information security awareness will be the inevitable measures to prevent and control information security.

Research on the protection of personal information in China started relatively late. The introduction of the Personal Information Protection Law is an important part of the process of personal information protection in China. The Personal Information Protection Law not only laid the foundation of a new law for personal information protection in China, but also became a fundamental legislation in the digital context [3]. The implementation of the Personal Information Protection Law has been widely followed, mostly from theoretical level analysis by Guo Feng, Chen Longye, and Jia Yuhui [4] and current news in newspapers by Gao Xiaoping and Ye Dan [5], as well as from specific industries to study the impact of the implementation of the Personal Information Protection Law on related industries, such as the medical industry [6], the financial industry [7], etc.

The results of expert data analysis show that users' perceived threat, privacy concerns, response efficacy and self-efficacy on the Internet will have a direct positive impact on personal information security privacy protection intention. Response cost will have a negative impact on users' protection intention; personal information security privacy protection intention is the mediating variable of the whole influence factor model, and the rest of the exogenous potential variables have an indirect influence on protection behavior. Jia Ruonan, Wang Jiewei, and Fan Xiaochun (2021) [8] pointed out that response efficacy, self-efficacy, response cost, perceived threat, and privacy concern have significant direct effects on users' willingness to protect personal information security privacy, in which response cost plays a negative role, and the above five variables indirectly affect users' protection behavior through the mediating variable willingness to protect. By considering the factors influencing the willingness to protect personal meaning on the Internet among them, we believe that privacy concern, perceived threat and self-efficacy all have some degree of influence on the degree of residents' willingness to protect their privacy on the Internet platform.

To sum up, by summarizing the relevant literature at home and abroad, we can find that people pay more and more attention to the issue of personal information security in the big data environment, and the series of suggestions and countermeasures they put forward are of reference significance for this study. In the research of personal information security issues, scholars fully realize the serious harm caused by the chaos of personal information security to citizens and society, and point out the importance of platform responsibility awareness, governmental supervision, enterprise self-regulation and citizens' legal awareness to personal information protection in the research of the dilemma and the way out after the introduction of the Personal Information Protection Law respectively. At present, domestic academics mainly analyze the issue of personal information security from the level of laws and regulations, stand in the unilateral perspective of laws to protect personal information security, and put forward corresponding suggestions and countermeasures for the improvement of laws and regulations, such as improving legislation related to personal information security, formulating and improving the system, optimizing the implementation conditions, clarifying the scope of acceptance, fully reflecting the effectiveness of the class action law, and providing a clear understanding of the concept of "personal information security". The concept of "personal information security" is clearly defined and the elements of the damage to rights and interests are sorted out, but there is little empirical research on the effectiveness of the implementation of the Personal Information Security Law.

2.2 Research hypothesis

Through the review of the existing literature, it is found that there are numerous factors that affect residents' willingness to protect privacy, i.e., including subjective factors as well as external environmental factors. Therefore, the scale selected for this paper and the framework of questionnaire design refer to Jia Ruonan, Wang Jiewei and other scholars (2021) [8] "Research on the factors influencing the privacy protection behavior of personal information security of social network users" and "Research on the factors influencing consumer information disclosure behavior in e-commerce" [9] and on this basis, the research hypothesis is modified according to the real research object to form this paper's research model.

Self-efficacy, and privacy concerns and willingness to protect privacy

Bandura A defines self-efficacy as "an individual's perceptions and beliefs about his or her ability to perform specific tasks and achieve specific goals". In the field of sociology, self-efficacy is often used to explain how individuals primarily feel about their behavior and individual behavioral problems [10]. In general, individuals with high self-efficacy are more confident and will work harder to complete tasks. Many studies have shown that self-efficacy has a significant positive effect on behavioral intentions to protect private information in different contexts [11]. Users with higher self-efficacy perceptions are more confident in their ability to protect their self-privacy, as well as in their ability to effectively prevent personal privacy leakage, and their willingness to protect privacy will be stronger. Therefore, the first hypothesis proposed in this paper is that:

H1: Self-efficacy positively influences the willingness of individuals to protect their privacy.

Risk perception, as a subjective judgment of the negative consequences and severity of an event, is also an important indicator to study people's uncertainty and psychological fear of a particular event. Research shows that when users perceive an increased risk of personal privacy information infringement, they are more inclined to take positive protection measures to protect their own rights and interests [12]. If users believe that there is a high risk of personal privacy information leakage, but the leakage risk will not bring serious losses or impacts, they tend to give up the protection of their privacy. That is, risk perception plays a positive role in the willingness to adopt protection behaviors. Therefore, the second hypothesis proposed in this paper is that:

H2: Risk perception positively influences individuals' willingness to protect their privacy.

The contradiction between the use of personal information and the protection of privacy has led to an increasing interest in the issue of personal privacy information in society and science, and thus has generated many empirical studies related to privacy concerns and privacy self-disclosure [13]. Related theories propose that privacy concern is a perception and awareness related to privacy disclosure, a subjective feeling about the information environment in which individual lives [14], and privacy concern refers to the user's sensitivity and concern about the handling, collection, and use of his or her private information, which reflects the user's subjective feeling about the environment in which the information lives. In the activities of the Internet, privacy concern is positively related to the willingness to protect personal privacy. Therefore, the third hypothesis proposed in this paper is that:

H3: Privacy concerns positively influence residents' willingness to protect their personal privacy.

Reactive efficacy and privacy invasion experience and willingness to protect privacy

Reactive efficacy refers to the degree to which individuals perceive their own behavior and are concerned about whether the results of their behavior will benefit them. That is, users are more willing to actively adopt their own behavior if they believe it will protect their rights and interests. Surveys have shown that if users perceive that security technology software is effective in protecting their information and reducing the risk of privacy breaches, they are more likely to use these technology tools and security measures to protect their privacy [15]. Many experimental studies have shown that response effectiveness has a positive effect on privacy protection in many scenarios. Therefore, the fourth hypothesis proposed in this paper is that:

H4: Response efficacy positively influences the willingness to protect the privacy of personal information security.

Privacy violation experience refers to the experience of personal privacy information leakage and misuse that residents have suffered when they were active on the Internet platform. By starting with residents' personal or family and friends' violation experiences, we can understand whether there is or has occurred a situation of personal information security threat around residents [16]. Generally speaking, if the degree of privacy invasion around the residents is greater, they will pay more attention to the protection of personal privacy. Some studies show that people will pay more attention to personal a privacy protection and will have a stronger willingness to protect themselves after they have experienced privacy invasion. Therefore, the fifth hypothesis proposed in this paper is that:

H5: Privacy violation experience positively influences willingness to protect personal information security privacy.

Knowledge of privacy willingness to protect privacy

Privacy knowledge refers to the degree of residents' knowledge about privacy in their activities on the Internet platform. By collecting residents' knowledge about national privacy-related policies and systems, their opinions on how to protect their privacy and how to timely defend their rights when their privacy is violated, we can conclude that the degree of privacy knowledge has a strong or weak effect on residents' willingness to protect themselves [17]. As for the ways to protect personal privacy, if residents have sufficient knowledge about self-privacy protection when they conduct online activities, they will strengthen the protection of their own information; finally, when their privacy rights are violated, residents will be better informed about various channels to defend their rights. Finally, when personal privacy is violated, residents will be better able to protect and ensure the security of their own information if they are aware of the various channels to defend their rights [18]. Therefore, the sixth hypothesis proposed in this paper is that:

H6: The degree of privacy knowledge positively influences the willingness to protect personal information security privacy.

2.3 Research model

Based on the above assumptions, this paper constructs a model of factors influencing residents' willingness to protect privacy in the context of the Personal Information Protection Law, as shown in **Figure 1**:

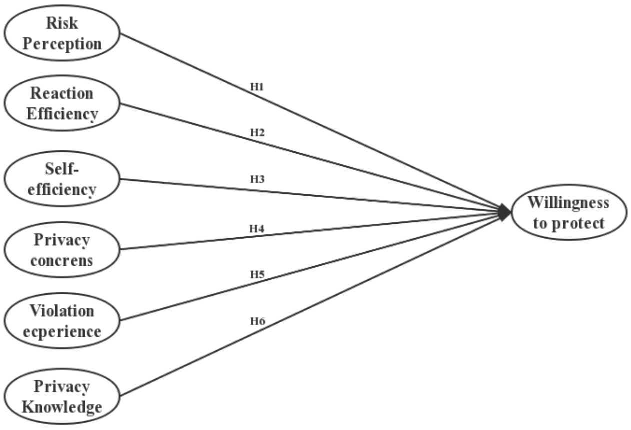

Figure 1. Model of factors influencing residents' willingness to protect personal privacy.

3. Study variable design and data acquisition

3.1 Study variable design

In order to reduce the multicollinearity among the six factors that influenced the data analysis and to better evaluate the influencing factors that affect the willingness to protect privacy in digital marketing, the questionnaire was intentionally designed to categorize the six factors: risk perception, response efficacy, self-efficacy, privacy concerns, and experience of violation [18,19]. When measuring this factor, all factors were quantified using a five-point Likert scale, except for measuring the frequency of monthly online purchases, which was measured numerically. The specific quantification is shown in **Table 1**.

3.2 Data acquisition

In order to cooperate with the local epidemic prevention and control work and to improve the efficiency of the survey, this study mainly adopted the online survey method, using the questionnaire platform "Questionnaire Star" to conduct the survey. 530 questionnaires were collected, and the recovery rate was 100%. In order to understand the current situation of residents' willingness to protect their privacy in relation to the introduction of the Personal Protection Law, the author adopted a multi-stage sampling method and selected 530 residents from five districts of Foshan City, Guangdong Province as survey respondents, taking into account various factors such as gender, age, education level and occupation of the survey respondents to cover the whole group of residents. The age of the respondents was mainly distributed between 18-40 years old, in line with the age distribution of high frequency Internet users; 143 respondents were male and 387 were female, accounting for 27.0% of males and 73.0% of females; the largest number of respondents were educated to bachelor degree or above, accounting for over 90%; the respondents' occupations were widely distributed, including students, teachers, white-collar workers, lawyers, doctors, etc, The respondents' occupations are widely distributed, including students, teachers, white-collar workers, lawyers, doctors, etc. This shows that the sample of this study has a high coverage and rich experience in Internet use, and is highly representative.

The city of Foshan is the location of the research object, and only collecting data from this region is to

Table 1. Scale design.

Factor categorization	Indicators	Quantification criteria
Privacy concerns	Residents' attitudes towards privacy breaches	5 4 3 2 1 Very high Very low
	Residents' concerns about the safety of online shopping	
	Residents' attitudes towards personalized recommendations Residents' attitudes towards privacy policies	
Risk perception	Residents' fear of privacy breach level	5 4 3 2 1 Strongly agree Strongly disagree
	Residents' attitudes towards filling in personal information for online purchases	
	Residents' perceptions of financial losses from online privacy breaches Residents' views on the misuse of personal information	
Reaction efficiency	Perceptions of security measures to reduce risk	5 4 3 2 1 Strongly agree-Strongly disagree
	Opinions on regular data backup	
	Opinions on setting complex passwords	
Self-efficacy	Confidence in online shopping to avoid privacy breach	5 4 3 2 1 Very confident-Very unconfident
	Confidence in the use of security measures to protect privacy	
	Confidence in identifying hazards	
Privacy violation experience	Extent of privacy violations	5 4 3 2 1 Very high Very low
	Greater emphasis on the degree of privacy protection	
	Trust in online shopping	
Level of knowledge understanding	Knowledge of laws and regulations	5 4 3 2 1 Very well understood-Very poorly understood
	Understanding of protection methods	
	Understanding of the right to defend	
Willingness to protect	Security measures to protect personal privacy	5 4 3 2 1 Very high Very low
	Personal privacy use environment	

obtain more authentic and reliable research results, because the data from this region are easier to obtain and confirm, and also more representative and comparable. Foshan City is a typical case or representative region of the research object, and the choice of collecting data only from this region allows for a more in-depth analysis of its characteristics, patterns, strengths and weaknesses, and has greater research value and practical significance.

4. Analysis of data results

4.1 Basic analysis of the scale

Scale description statistics

Descriptive statistics of specific scales are shown in **Table 2**. In order to understand the basics of the scale, the minimum, maximum, variance, and standard deviation of the seven factors of privacy concern, risk perception, response efficacy, self-efficacy, privacy violation experience, privacy knowledge, and willingness to protect were calculated. Since the scale is designed to measure respondents who have used e-commerce for shopping, the statistics of the scale are selected from those who have used the Internet for shopping within one month. The analysis of the above data shows that most of the residents show high proportions of privacy concern, risk perception, response efficacy, self-efficacy, privacy violation experience, self-efficacy and willingness to protect privacy, while privacy knowledge, i.e., knowledge of privacy laws such as the Personal Protection Law, is still at a moderate level, indicating that the residents still need to improve in terms of privacy knowledge.

Table 2. Scale descriptive statistics.

	Number of cases		**Standard deviation**	**Variance**	**Minimum value**	**Maximum value**
	Effective	**Missing**				
Attitude to privacy breach	530	0	0.821	0.674	1	5
Privacy and security attitude	530	0	1.046	1.094	1	5
Personalized recommendation attitude	530	0	1.001	1.002	1	5
Privacy policy attitudes	530	0	1.111	1.234	1	5
Privacy breach fear level	530	0	0.881	0.777	1	5
Fill in personal information attitude	530	0	0.934	0.872	1	5
Economic loss	530	0	0.905	0.819	1	5
Improper use of information	530	0	0.954	0.911	1	5
Security measures to reduce information security risks	530	0	0.93	0.865	1	5
Backing up data to improve information security	530	0	0.987	0.973	1	5
Complex passwords to prevent information data leakage	530	0	0.945	0.893	1	5
Ability to avoid information leakage	530	0	0.924	0.854	1	5
Degree of confidence in protecting personal privacy	530	0	0.915	0.838	1	5
Level of confidence in identifying and responding correctly	530	0	0.948	0.899	1	5
The severity of the invasion of personal privacy experience	530	0	0.924	0.854	1	5
Valuing the protection of personal privacy after violation	530	0	0.926	0.858	1	5
Trust in online shopping after experiencing privacy violations	530	0	0.864	0.746	1	5
Level of knowledge of privacy protection laws	530	0	0.99	0.981	1	5
Channels to protect personal privacy	530	0	0.955	0.912	1	5
Ways to defend your rights	530	0	0.98	0.961	1	5
Willingness to use security measures to protect personal privacy	530	0	0.965	0.93	1	5
Relevant departments to regulate the use of personal privacy environment	530	0	0.919	0.845	1	5
Personal information filled in when registering for an account	530	0	0.978	0.956	1	5

Analysis of respondents' suggestions for participation in decision making

Among the issues of how to strengthen the privacy protection of Internet platforms, a large proportion of them choose to improve the restriction of laws and regulations, strengthen the management of network security, industry self-discipline and corporate responsibility. Respondents are more inclined to accept the above three ways to improve privacy security in Internet platforms (**Table 3**). Online consumers hope that the state and government can strengthen supervision to ensure the security of personal privacy in online platforms. They hope that through legislation, severe punishment and other ways to restrict the arbitrary violation of personal privacy of the business, improve online privacy security. Therefore, the government should implement management and supervision of network privacy security policies from the perspective of maintaining user privacy security, so that users have no worries when using the corresponding products [19].

At the same time, online consumers hope that e-commerce merchants can achieve industry self-dis-

Table 3. Analysis of surveyors' suggestions for participation in decision making.

Question	Options	Frequency	Percentage (%)
How to strengthen privacy protection in Internet platforms	The state to strengthen the regulation of enterprises	94	17.8
	Improve laws and regulations to restrict	71	13.44
	Education to raise awareness of protection	46	8.69
	Strengthen network security management	101	19.13
	Industry self-regulation and corporate responsibility	124	23.42
	Other	34	6.52

cipline and assume social responsibilities and obligations as enterprises. Precision marketing is scattered across industries, so the power of a single company to change user privacy protection is limited. However, if the various enterprises can coordinate the "unified pace", the results may be considerable. Therefore, we should try to promote enterprises to form a consensus on privacy protection through industry associations, formulate more unified policy standards, and gradually form industry standards, so as to promote privacy protection in a wider scope [20]. In this process, leading companies should be encouraged to improve their privacy policies, disclose their user data collection and use to the public, and encourage them to report violations of information collection and processing by other companies in the industry. Such practices can practice corporate social responsibility and promote the industry as a whole to improve the level of privacy protection.

4.2 Reliability and validity analysis of the questionnaire, factor analysis

In order to understand the degree of change in the willingness of residents to protect their privacy information after the introduction of the Personal Protection Law and the existence of relevant factors, this paper conducts factor analysis on each factor to see whether it is suitable for modeling. By investigating the influence of the factors on each other, we investigate the influence of users' willingness to protect their privacy and their expectation of privacy protection.

Reliability analysis

The effect of Cronbach's alpha coefficient worth range as well as reliability: 0.80 to 0.90 very good 0.70 to 0.80 quite good; 0.65 to 0.70 minimum acceptable value; 0.60 to 0.65 best don't; this analysis was done using SPSS data analysis and we got Cronbach's alpha coefficient value of 0.863, which is in the very good range, so **Table 4** shows that the questionnaire reliability is quite good, which can provide great help and good analysis for our subsequent research.

Table 4. Clonbach Alpha **Table 1**.

Reliability statistics	
Cronbach Alpha	Number of items
0.863	23

The Cronbach's alpha coefficients for the variables studied in this paper, privacy concern, risk perception, response efficacy, self-efficacy, experience of privacy violation, knowledge of privacy, and willingness to protect, were 0.850, 0.752, 0.723, 0.791, 0.793, 0.847, and 0.741, respectively, all of which were greater than the criterion of 0.7, indicating that the variables set have good inter The internal consistency of the variables. Specific data are shown in **Table 5**.

Table 5. Clonbach Alpha.

Factors	Number of projects	Cronbach's alpha
Privacy concerns	4	0.850
Risk perception	4	0.752
Reaction efficiency	3	0.723
Self-efficacy	3	0.791
Privacy violation experience	3	0.793
Level of knowledge of privacy	3	0.847
Willingness to protect	3	0.741

Validity analysis, factor analysis

In order to understand the degree of change in the willingness of residents to protect their privacy information after the introduction of the Personal Protection Law and the existence of relevant factors, this paper conducts a factor analysis of each factor to see whether it is suitable for modeling. By investigating the influence of the factors on each other, we investigate the influence of users' willingness to protect their privacy and their expectation of privacy protection.

Exploratory factor analysis can distinguish the structure of items by verifying the factor relationships among the items of the scale and reflecting the structural validity of the questionnaire. The suitability of items for factor analysis can be determined by the magnitude of the KMO and Bartlett's sphericity test. The KMO reflects the correlation and bias between the items and has an indicator value between 0 and 1. By Bartlett's spherical test, we judge whether the correlation matrix of the variables is a unit matrix or not, and the final test results are presented in the table below. The final test results are shown in **Table 6**.

Table 6. KMO test and Bartlett's sphericity test table.

KMO and Bartlett's test		
KMO Sampling suitability quantity		0.838
Bartlett's sphericity test	Approximate cardinality	2027.148
	Degree of freedom	253
	Significance	0.000

To analyze the validity of the questionnaire, by analyzing the KMO value, if the KMO value is higher than 0.8, it indicates that the validity of the questionnaire is high; if it is between 0.7 and 0.8, it indicates that the validity is good; if it is in the range of 0.6 to 0.7, it indicates that the validity is barely acceptable; if the value is less than 0.6, it proves that the questionnaire has poor validity. From the SPSS analysis, the KMO value of the questionnaire is 0.838, which belongs to high validity and is suitable for factor analysis.

Based on the above tests, for this analysis, we used these factors for further statistical analysis (**Table 7**).

Since the loadings matrix structure of the evaluation index is complex and cannot be used to explain realistic problems, this paper introduces the maximum variance rotation method to construct the principal component matrix. The factor loading matrix after the rotation will be differentiated, which is beneficial to explain the economic significance of the factors, and this paper adopts the principle of factor coefficient retention greater than 0.5 methods. After measurement, principal factor 1 has higher loadings in terms of knowledge of privacy protection laws, channels to protect personal privacy, and methods to defend rights, etc., which we call the privacy knowledge factor according to the previous assumptions; principal factor 2 has higher loadings in terms of ability to avoid information leakage, self-confidence in protecting personal privacy, and self-confidence in identifying and responding correctly. The main factor 3 has high loadings on attitude toward filling out personal information, causing financial loss, and improper use of information, which we call the risk perception factor according to the previous hypothesis; the main factor 4 has high loadings on willingness to use security measures to protect personal privacy, the relevant authorities to regulate the environment of personal privacy use, and personal information filled out when registering for an account, which we call willingness to protect according to the previous hypothesis. We call it the willingness to protect factor according to the previous hypothesis; principal factor 5 has higher loadings in privacy disclosure attitude, privacy security attitude, etc., and we call it the privacy concern factor according to the previous hypothesis. Overall, the higher loading factors extracted from the rotated principal component matrix are fully consistent with the originally expected hypothesis.

4.3 Validation factor analysis

Std. Estimate is used to indicate the correlation between the factor and the analyzed item, generally significant and the value of Std. Estimate is greater than 0.7, it indicates a strong correlation between the factor and the analyzed item; if the item does not

Table 7. Rotated component matrix.

Component matrix after rotation						
Evaluation indicators	**Ingredients**					
	1	**2**	**3**	**4**	**5**	**6**
Attitude to privacy breach					0.814	
Privacy and security attitude					0.806	
Personalized recommendation attitude						0.738
Privacy policy attitudes						0.612
Privacy breach fear level					0.580	
Fill in personal information attitude			0.709			
Economic loss			0.731			
Improper use of information			0.754			
Security measures to reduce information security risks						
Backing up data to improve information security		0.637				
Complex passwords to prevent information data leakage						
Ability to avoid information leakage		0.780				
Level of confidence in protecting personal privacy		0.655				
Level of confidence in identifying and responding correctly		0.615				
The severity of the invasion of personal privacy experience	0.588					
Valuing the protection of personal privacy after violation				0.563		
Trust in online shopping after experiencing privacy violations	0.671					
Level of knowledge of privacy protection laws	0.734					
Channels to protect personal privacy	0.797					
Ways to defend your rights	0.778					
Relevant departments to regulate the use of personal privacy environment				0.721		
Personal information filled in when registering for an account				0.768		

Extraction method: Principal component analysis.

Rotation method: Kaiser normalized maximum variance method.

a. The rotation converges after 8 iterations.

show significance, or the Std. Estimate is low (if it is lower than 0.4), it indicates a weak relationship between the item and the factor. is weak. The data analysis shows that the inter-factor relationship of this survey is strong, and most of the Std. Estimate is at 0.7, which is significant. Specific data are shown in **Table 8**.

4.4 Correlation analysis and differential validity

In this study, we used the HTMT method (heterogeneous-monogeneous ratio) in **Table 9** for discriminant validity verification; first, the values in the table indicate the HTMT values between two factors; sec-

Table 8. Validation factor analysis table.

Factor (latent variable)	Title	Non-standard load factor (Coef.)	Standard error (Std. Error)	*z* (CR value)	*p*	Standard load factor (Std. Estimate)
Privacy concerns	PC1 PC2. PC3 PC4	1.000	-	-	-	0.753
		0.944	0.067	14.005	0.000	0.729
		1.026	0.076	13.497	0.743	0.706
		1.221	0.143	8.539	0.000	0.813
Risk perception	RP1	1.000	-	-	-	0.664
	RP2	1.052	0.131	8.020	0.000	0.645
	RP3	0.947	0.123	7.690	0.000	0.612
	RP4	1.113	0.131	8.513	0.000	0.697
Reaction efficiency	RE1	1.000	-	-	-	0.634
	RE2	1.133	0.136	8.321	0.000	0.706
	ER3	1.193	0.143	8.371	0.000	0.713
Self-efficacy	SE1	1.000	-	-	-	0.709
	SE2	1.121	0.111	10.074	0.000	0.774
	SE3	1.068	0.107	9.983	0.000	0.764
Privacy violation experience	PI1	1.000	-	-	-	0.572
	PI2	0.908	0.146	6.239	0.000	0.556
	PI3	0.670	0.143	4.681	0.000	0.382
Privacy Knowledge	PK1	1.000	-	-	-	0.765
	PK2	1.026	0.086	11.884	0.000	0.793
	PK3	1.087	0.086	12.697	0.000	0.863
Willingness to protect	PB1	1.000	-	-	-	0.776
	PB2	0.765	0.100	7.679	0.000	0.585
	PB3	0.923	0.102	9.026	0.000	0.751

Table 9. HTMT results table.

	Privacy concerns	Risk perception	Reaction efficiency	Self efficacy	Privacy violation experience	Privacy knowledge	Protection intention
Privacy concerns	-						
Risk perception	0.721	-					
Reaction efficiency	0.495	0.729	-				
Self-efficacy	0.498	0.319	0.648	-			
Privacy violation experience	0.560	0.657	0.655	0.695	-		
Privacy knowledge	0.300	0.276	0.411	0.686	0.778	-	
Willingness to protect	0.614	0.445	0.549	0.111	0.326	–0.002	-

ond, in general, HTMT values less than 0.85 indicate discriminant validity between two factors; and all the HTMT values in the table are within the standard range, which is sufficient to indicate that the variables in this analysis have good discriminant validity.

5. Conclusions and recommendations

This study explores the changes in residents' willingness to protect their own privacy in the context of the Personal Information Protection Law by analyzing the factors influencing users' willingness to protect their privacy behavior, and comparing the degree of influence involving different factors on the willingness to protect. The research findings obtained from this study are analyzed as follows:

Risk perception had a significant positive effect on willingness to protect (F = 7.885, $p < 0.05$), privacy concern (F = 9.059, $p < 0.05$) positively influenced willingness to protect privacy, and response efficacy (F = 10.674, $p < 0.05$) positively influenced willingness to protect privacy, i.e., the findings of H1, H2, and H3 were consistent with expectations, and consistent with the traditional theory of planned behavior. It indicates that when users conduct digital transactions and information output on Internet platforms, residents are able to make appropriate protection measures with the perceived risks in digital transactions and online consumption. Moreover, users who are concerned about privacy information are more sensitive to the leakage of personal information and act promptly to ensure their privacy security. In addition, self-efficacy (F = 6.127, $p < 0.05$), invasion experience (F = 12.457, p =< 0.05) and knowledge of privacy (F = 8.237, $p < 0.05$) positively affect the willingness to protect privacy, i.e., H4, H5 and H6 hold, indicating that as an individual user in the Internet platform activities to privacy threats and privacy violations. The degree of confidence in self-protection and the degree of knowledge about it are factors that directly affect users' willingness to protect. H5 holds that the experience of privacy violation positively affects the willingness to protect privacy, and the relevant data prove that the group with privacy violation has a stronger willingness to protect personal privacy.

In summary, when users engage in digital transactions and information output on internet platforms, they need to be vigilant about risks, pay attention to privacy issues, and believe in their protective ability and effectiveness, as well as possess basic privacy knowledge. These factors can have a positive impact on an individual's willingness to protect privacy. Meanwhile, users who have experienced privacy violations will have a stronger willingness to protect their personal privacy. These conclusions are consistent with the traditional Theory of planned behavior, and provide some suggestions for individuals to protect their privacy on the Internet platform.

Based on relevant professional literature and statistical analysis of research data, we have come up with the following recommendations:

(1) Legal aspects

First, construct a "data trust" system to realize the normal flow of information and data on the basis of data security.

According to the data analysis, the higher the self-efficacy, the stronger the privacy protection of individual residents, i.e., when residents realize that self-protection is more effective, they will be more proactive in using these methods to protect their privacy and security. Our law can balance the sharing of user information and data with the operators' need to use the data in a transactional manner by constructing a "data trust" system. In June 2022, the EU introduced the Data Governance Act ("DGA"), which introduced the concept of data intermediaries for the first time. The EU data intermediary service providers are neutral data intermediaries, and by separating the data provision, intermediation and use aspects of data transactions, the relationship between the two parties in a data transaction is changed to a tripartite relationship. to enhance society's trust in data intermediary services, facilitate the sharing and circulation of data, and promote the building of an emerging data-driven ecosystem. For ordinary users, this means that personal information and data will be managed through public servers or relevant data trusts. When enterprises need to use the data, they can use trusts to obtain the data, and while protecting the security of user information, users will be able to obtain certain "data dividends". Under the framework of the Personal Information Protection Law, China should pay attention to the resolution of personal trust issues, incorporate data issues into the public issues of society, encourage the establishment of data agencies and other diversified third-party data service institutions, and also be brave enough to revise and seek the most suitable data sharing model for China.

Second, in the pursuit of balanced legal liability settings, strict legal liability must be matched with flexible enforcement mechanisms.

In order to promote the normal and reasonable flow of data, the law should have a sufficient deterrent effect for each network platform, i.e., the law can enhance the cost of violation of the law through a high fine system, thus prompting enterprises to establish a good internal data standardization system and realize the cooperation of "enterprise autonomy + government regulation" to create a safe network atmosphere. Governance. At the same time, a strict legal system must be combined with a flexible law enforcement mechanism, experts proposed the construction of an administrative law enforcement settlement agreement system, enterprises through the establishment of a sound and compliant data processing system as a condition for administrative law enforcement settlement, and timely disclosure of the enterprise's situation to the community, the provisions of a certain assessment period, allowing enterprises to have the opportunity to rehabilitate.

Third, avoid "objectification of data subjects".

In the data analysis, we can learn that the higher the level of privacy concern of the residents, the stronger their willingness to protect privacy, so the relevant law should focus on the subjectivity of the data subject when setting the "privacy consent policy", so that the subject is aware of their own privacy information issues, and indirectly increase the degree of willingness to protect their own privacy. In the Personal Protection Law, the premise of "inform-consent" is that every data subject is a rational person who reads and understands each privacy policy statement in detail and makes a final decision on whether to provide his or her personal information to the platform. However, in reality, this is almost impossible to achieve, and many operators are currently taking advantage of this phenomenon to hide the privacy rules. It is found that the problem of "objectification of data subjects" exists in all major platform software, which is due to the information asymmetry between users and operators, resulting in users not being able to understand how operators collect, process and even trade and share their personal information, not to mention the control of their own information data. The user, as the subject of the information, is in a passive and blind "object" position in the handling and selection of his personal information. The Personal Protection Law needs to make a clear distinction between express consent and implied notice. For important privacy and sensitive information of users, special emphasis should be placed on operators giving "express consent" to users, while for the general personal information of users, operators can handle it through "implied notice", focusing on the commercial use of information processing. The commercial use of the specifications.

Fourth, the construction of network data leakage notification institutional mechanism

Based on the results of the data analysis, we conclude that risk perception has a positive impact on privacy protection intention. When the information data is leaked, the notification is fed back to the user, which not only enhances the user's perceived risk of personal privacy information leakage, but also is a protective behavior for the user's privacy information, which can, to a certain extent, increases the user's willingness to protect their privacy information and enhance privacy protection behavior. The current existing legal system still does not have a strong and effective method to solve the problem of frequent privacy leaks. In reference to numerous literature, this paper believes that national legislation can be observed by constructing an institutional mechanism for notification of network data leaks, and making legal observations in the whole process and in each link of data activities. Clarify the remedial measures and obligations that network operators should take in case of information leakage of user information data occurs or may occur, and when the danger level of data leakage reaches a certain index, they should promptly notify users and relevant management personnel through various ways, and promptly take effective measures to organize further deterioration of information leakage. At the same time, the platform companies that do not timely fulfill the relevant notification obligations and legal responsibilities are given severe penalty provisions. On the other hand, the law should also make clear and explicit provisions on the severity of information leakage and related indicators to enhance the operability of users, operators and the government's three parties.

(2) Corporate level

First, strengthen the openness and transparency of data decision-making, and achieve timely and accurate information updates.

The introduction of the Personal Information Protection Law marks a new historical stage of personal information protection with the authority of the law, no longer the previous rough and tumble management, but more refined and standardized requirements and instructions for information collectors and processors. Emphasize that when enterprises carry out personal information protection, they should adhere to the protection of data information decision-making openness and transparency, whether it is to do big data analysis, assist decision-making, marketing and promotion, should try to be open and transparent, transparent details, rather than a generalization. The handling of user data can be made transparent through privacy policy agreements, methods that can be inquired at any time, etc. to ensure that users have the right to freely dispose of and understand their own private information, and accept the supervision and management of the user public. Regular updates to ensure the accuracy and completeness of information This can, to a certain extent, address residents' fear of self-privacy leakage and abuse, and at the same time can raise the concern of self-privacy information, and thus better protect their privacy information from infringement.

Second, improve the privacy statement and resolve the inherent paradox of informed consent.

By improving the comprehensibility of the privacy statement, we can enhance residents' understanding of the laws and regulations related to privacy information and, therefore, their willingness to protect their own privacy information. Most websites, application platforms, and social media currently provide a privacy statement user agreement or policy that demonstrates the platform's commitment to the proper use of user privacy. But users rarely make the choice to disagree when faced with a privacy agreement unless they give up using the feature or service, and for this reason, most users will blindly agree to the privacy agreement rather than read the privacy policy beforehand. Moreover, many jurists may not be able to distinguish the pitfalls of the form contracts in the platforms, let alone ordinary users. Moreover, such electronic format contracts are not supplemented by opinions from the personal side, and individual users cannot fully bind themselves according to the terms of the privacy statement, for which reason, the situation of user privacy protection is very serious.

In order to make users better understand the content of the "Privacy Agreement", the platform should introduce a privacy policy that is suitable for most users to read, and should minimize the use of remote jargon in the statement, so that ordinary users can easily read and understand the content of the agreement, which not only improves the level of understanding of users, but also truly protects the user's privacy.

Third, strengthen user collaboration and establish a monitoring platform.

According to the analysis, it is concluded that privacy concern has a positive impact on residents' willingness to improve personal information protection, then it can be achieved by improving residents' privacy concern and thus their willingness to improve privacy protection. To this end, the role of Internet users can be brought into play in the new environment with a large system of Internet users and a severely overloaded information environment, and a user monitoring platform can be established to allow the majority of users to participate in the monitoring team and assume the responsibility of monitoring society. Furthermore, users can also participate in information screening and review as a new supervisory board, pay attention to various illegal and irregular phenomena in the process of using the medium, and mark and report content that violates and abuses others' privacy through the platform's feedback system, so that the platform can more easily detect the behavior in the huge information flow, and thus better maintain the good environment of online social media platforms.

Fourth, regulate the behavior of enterprises and implement government laws and regulations.

The introduction of the Personal Information Protection Law provides a comprehensive, systematic and standardized legal basis for the protection of personal information privacy, the responsibility of information processors and the terms of reference of competent authorities. Residents are able to obtain a more systematic and powerful way to defend their rights in the face of infringements in the illegal collection and use of personal privacy information data, and to protect the collection, use, processing, provision, disclosure, deletion and other aspects of personal privacy information as well as specific scenarios such as the handling of sensitive personal information in a comprehensive manner. Due to the phenomenon of huge information inequality and asymmetry of rights between the platform and users, will lead most users to give up being more serious and complete the instructions requested by the platform in a step-by-step manner. For this reason, platforms should take national standards as a guide, update privacy statements in a timely manner, hire professional legal personnel to formulate as well as interpret relevant agreements, regulate their own behavior, implement the spirit of the national rule of law in detail, and work together to maintain social public safety.

(3) Individual level

First, strengthen individuals' awareness and ability to protect privacy.

Individuals should understand their privacy rights and learn how to take measures to protect their personal information. This includes using strong passwords, regularly updating software and applications, and carefully selecting platforms and channels for sharing personal information.

Second, be cautious in the collection and use of personal information.

When providing personal information, individuals should carefully read the privacy policy and terms, and ensure that they understand how personal information will be used and protected. Individuals can choose to only provide necessary information to avoid excessive sharing of sensitive personal information.

Third, regularly check and manage personal online accounts and privacy settings.

Individuals should regularly review their online accounts and ensure that privacy settings are appropriately configured. This includes restricting publicly available personal information, controlling the scope of personal information sharing, and regularly reviewing and deleting accounts and personal information that are no longer needed.

Fourth, be vigilant against online fraud and phishing attacks.

Individuals should be vigilant against fraudulent behavior and phishing attacks on the internet, and not easily click on suspicious links or download files of unknown origin. At the same time, individuals should remain vigilant and not easily disclose personal information to strangers or untrustworthy platforms.

Fifth, actively participate in privacy protection initiatives and activities.

Individuals can participate in relevant communities and organizations, support and promote privacy protection initiatives and activities. Through joint efforts, society can increase the importance of protecting personal privacy and promote internet platforms and related enterprises to pay more attention to user privacy security. Through personal efforts and awareness enhancement, individuals can effectively protect their privacy and contribute to the protection of privacy in society as a whole.

Conflict of Interest

There is no conflict of interest.

References

[1] Malandrino, D., Scarano, V., 2013. Privacy leakage on the Web: Diffusion and countermeasures. Computer Networks. 57(14), 2833-2855.

[2] Baruh, L., Secinti, E., Cemalcilar, Z., 2017. Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication. 67(1), 26-53.

[3] Long, W.Q., 2021. "Ge ren xin xi bao hu fa" de ji ben fa ding wei yu bao hu gong neng—ji yu xin fa ti xi xing cheng ji qi zhan kai de fen xi (Chinese) [The basic law positioning and protection function of the Personal Information Protection Law: An analysis based on the formation and development of the new law system]. Modern Law. 43(5), 84-104.

[4] Guo, F., Chen, L.Y., Jia, Y.H., 2022. "Ge ren xin xi bao hu fa" ju ti shi yong zhong de ruo gan wen ti tan tao—ji yu "min fa dian" yu "ge ren xin xi bao hu fa" guan lian de shi jiao (Chinese) [Discussion on some problems in the specific application of the Personal Information Protection Law—Based on the perspective of the relationship between the Civil Code and the Personal Information Protection Law]. Journal of Applicable Law. (1), 12-22.

[5] Gao, X.P., Ye, D., 2021. Ge ren xin xi bao hu, hu lian wang qi ye zhun bei hao le ma? (Chinese) [Are Internet companies ready for personal information protection?]. Nanfang Daily. (16), 26-27.

[6] Wu, L.F., 2002. "Ge ren xin xi bao hu fa" shi shi xia de yi liao shu ju guan li he ying yong tan tao (Chinese) [Discussion on medical data management and application under the implementation of Personal Information Protection Law]. Soft Sciences of Health. 36(1), 5-7.

[7] Zhang, K., 2021. "Ge ren xin xi bao hu fa" dui bao xian hang ye de ying xiang yu ying dui jian yi (Chinese) [The impact of the Personal Information Protection Law on the insurance industry and countermeasures]. Tsinghua Financial Review. (12), 88-92.

[8] Jia, R.N., Wang, X.W., Fan, X.Ch., 2001. She jiao wang luo yong hu ge ren xin xi an quan yin si bao hu xing wei ying xiang yin su yan jiu (Chinese) [Research on influencing factors of personal information security and privacy protection behavior of social network users]. Modern Information. 41(9), 105-114+143.

[9] Chen, Q., 2021. Yi dong duan shi pin ying yong zhong de gong min yin si quan bao hu yan jiu (Chinese) [Research on the protection of citizens' privacy in mobile short video applications] [Master's thesis]. Nanchang: Jiangxi University of Finance and Economics.

[10] Wang, L.M., Ding, X.D., 2021. Lun "ge ren xin xi bao hu fa" de liang dian, te se yu shi yong (Chinese) [On the highlights, characteristics and application of Personal Information Protection Law]. Jurist. (6), 1-16+191.

[11] Xiong, C.L., Tong, Y.Q., 2021. Bian jie yu ping heng: ge ren yin si xin xi bao hu zhong de shu ju zhi li lu jing yu si kao (Chinese) [Boundary and balance: The path and reflection of data governance in personal privacy information protection]. Science and Technology Communication. 13(24), 64-68.

[12] Wu, S.X., 2022. Da shu ju bei jing xia ge ren yin si bao hu de fa lü gui zhi (Chinese) [Legal regulation of Personal Privacy Protection in the background of big Data]. Regional Governance. 20, 0093-0096.

[13] Zhu, G., Li, F.J., Shen, Y.M., et al., 2022. She jiao mei ti yin si zheng ce de yue du yi yuan yan jiu—ji yu TAM mo xing yu zi wo xiao neng li lun shi jiao (Chinese) [A study on reading intention of social media privacy policy—based on TAM model and self-efficacy theory perspective]. Modern Intelligence. 42(1), 150-166.

[14] Zheng, Y., Shi, S., 2022. Chang jing qu dong: ge ren yin si bao hu sheng ji (Chinese) [Scene-driv-

en: personal privacy protection upgrade]. Intelligent Connected Vehicle. 2,62-67.

[15] Gao, Sh.Ch., 2000. Zi wo xiao neng li lun ping shu (Chinese) [A review of self-efficacy theory]. Psychological Development and Education. (1), 60-63.

[16] Yuan, X.L., Niu, J., 2021. She jiao mei ti yin si zheng ce yu yong hu zi wo biao lu de shi zheng yan jiu: yi ge bei tiao jie de zhong jie mo xing (Chinese) [An empirical study of social media privacy policies and user self-representation: A moderated mediation model]. Journal of Information Resource Management. 11(1), 49-58.

[17] Zhang, J.D., Jiang, L.P., 2021. Rong ru yong hu qun ti xing wei de yi dong she jiao wang luo yu qing chuan bo dong tai yan hua mo xing yan jiu (Chinese) [A dynamic evolutionary model of mobile social network opinion dissemination incorporating user group behavior]. Modern Intelligence. 41(5), 159-166+177.

[18] Tan, F., Yang, Y., Zhuo, Y.L., et al., 2021. Wang luo yin si zheng yi shi jian zhong yong hu yin si guan zhu ji qing gan dui bi yan jiu (Chinese) [A comparative study of users' privacy concerns and emotions in online privacy controversies]. Library and Information Work. 65(2), 87-97.

[19] Bandura, A., 1982. Self-efficacy mechanism in human agency. American Psychologist. 37(2), 122.

[20] Yang, X.W., 2009. Wang luo xin xi fu wu guo cheng zhong de ge ren yin si bao hu wen ti chu tan (Chinese) [A preliminary study on the protection of personal privacy in the process of network information service]. Inner Mongolia Science and Technology and Economy. (7), 445+449.