Asia Pacific Science Press

Asia Pacific Economic and Management Review
ISSN(O):3005-9275
ISSN(P):3005-9267
Vol. 2 No.2 (2025)

Research on the Tolerance of Privacy Leakage Among Consumers in Offline Retail Shopping Scenarios

Weizhen Wang[1], Minglei Li[2]*, Enyi Lai[3,4]

1.School of Business Administration, Jimei University -Keuka College Program, Xiamen, 361000, P.R.China

2.Faculty of Public Administration, Guangdong Vocational Institute of Public Administration, Guangzhou, 510800, P.R. China

3.Fujian Zhongdian Straits Institute of Intelligent Equipment, Xiamen, 361022, P.R.China

4.Faculty of Business, City University of Macau, Macau SAR, 999078, P.R. China

Corresponding author: Minglei Li, lml5270509@163.com

Abstract: With the continuous combination of artificial intelligence technology and the field of security, intelligent security is gradually popularized in offline retail scenes. While helping merchants to obtain and analyze consumer data and bringing certain consumption convenience to consumers, it also brings practical problems of privacy leakage. The CCTV 315 gala revealed the use of AI technology to obtain users' privacy information, helping consumers truly realize that they still need to protect their privacy information in the offline retail scene. By investigating the tolerance of privacy leakage in consumers' offline retail shopping scenarios, this paper hopes to explore how to better build a shopping environment between consumers and offline retail stores. After integrating the sensitivity of consumers' information type, the sensitivity of information receiving, information use sensitivity and related privacy theory, this paper developed and designed a third-order seventh scale. We collected data through questionnaire survey method, a total of 237 questionnaires were collected, and used to analyze the data and reliability test with SPSS software. The analysis proves that most consumers do not have a high tolerance for privacy leakage. Although there are differences between personalities, there is a centralized trend. Finally, this paper further reflects on how to build a better shopping environment and consumer experience of offline stores.

Keywords: Privacy Leakage; Consumer; Artificial Intelligence; Attitude Measurement

Published: Apr 24, 2025

DOI: https://doi.org/10.62177/apemr.v2i2.246

1.Introduction

1.1 Research Background

With the increasing popularity of artificial intelligence technology in the field of intelligent security, video surveillance has successfully broken through the boundaries of basic security functions, and more visual management and applications will become a reality. Traditional security focus on "see, see clearly", and has artificial intelligence technology blessing intelligence security, video monitoring positioning in how differentiation on the application, embodied in the matter, to advance analysis, these a series of intelligent security application of the ground, in increase convenience and commercial interests at the same time, also brought some privacy problems.3152021 party revealed Kohler bathroom, good shop, the morning stationery offline retailers for installed the Suzhou store palm network technology co., LTD., for information technology co., LTD., on the premise of consumers unaware, captured more than 3 million customer face information, and add labels to these consumers, in order to achieve the purpose of accurate marketing. Wandian palm “stealing” customers’ facial information, location information and other privacy behavior exposure, caused great panic and anger from all walks of life, as well as concerns about the security of personal privacy information. A group of offline retailers, led by Miniso and Xicha, were found to use such “cameras” to steal customers’ privacy information, such as facial information and location information, and the use is very common.

At present, there are many studies on the privacy protection of online Internet shopping, Volkswagen seems to think that online shopping involves information technology, In this, businesses and other personnel to obtain facial privacy information and other data; But in fact, in the offline retail scenario, Businesses are also using cameras like Wan, Constantly use AI technology to obtain people’s facial information, location information and other privacy during offline shopping, This paper hopes to discuss the issue of “tolerance of privacy leakage” in the attitude level of privacy concerns in the offline retail shopping scenario, To explore how to better build a better consumption environment between consumers and offline retail stores.

1.2 Research Questions and Significance

Current market demand oriented sales model, make enterprises pay more attention to consumer actual needs, at the same time with the increasingly widespread application of artificial intelligence technology, the improvement of cloud computing and the popularization of application, and the mature data mining technology, are related to obtain and analyze user data, understand the user preferences provides possible. For enterprises, collecting and analyzing user data can be used to analyze the market and study consumers, so as to fully tap the needs of consumers and obtain greater profits. However, the amount of information and data collected by users is not the better, on the one hand, when analyzing the huge amount of data, there may be insufficient analysis and high cost of daily maintenance; on the other hand, it also brings the risk of consumer satisfaction, moral and legal risks. Once the behavior of obtaining consumer privacy information is exposed, the trust of consumers in the corresponding enterprises will be greatly reduced. Faced with such a complex situation, the author tries to explore how to better build a shopping environment between consumers and offline retail stores by understanding the attitude of consumers about the tolerance of privacy leakage in the offline physical shopping scene.

For consumers, providing private information can be a double-edged sword. On the one hand, consumers may unknowingly disclose the privacy information they care about, causing the loss of their property or reputation; On the other hand, consumers may be willing to obtain some convenience through some privacy that individuals think is less important. But then it will bring new problems. For most consumers, which privacy information can be obtained by merchants in exchange for a certain extent of convenience, which privacy is their intention and is not allowed to be obtained by merchants, the author needs to explore this boundary, so as to build a harmonious and win-win shopping environment.

1.3 Study Methods

In order to solve the problems described above, the author tries to integrate quantitative analysis and qualitative analysis. Through sorting out relevant literature and the method of issuing questionnaires, the research is conducted according to the following methods and steps:

(1) Define the research objectives. By clarifying the privacy leakage incidents, understanding the public’s concerns about privacy, and sorting out relevant literature, we can understand the current situation of privacy leakage in the offline physical shopping scene, as well as people’s views on AI’s behavior of obtaining face privacy, and then determine the research target and build the corresponding framework.

(2) Determine the research methods. In view of the empirical research ideas and research risk tolerance methods, the author determines the methods of sorting out documents and issuing questionnaires.

(3) Refer to theoretical models, develop scales, and design questionnaires. Through sorting out the relevant literature, the author decided to draw on Adams ‘theory, and developed a scale and designed a questionnaire according to the author’s practical research problems.

(4) Questionnaire “probe trap” setting. The author considering the respondents may not patience to fill in the questionnaire, and research time urgent cannot test the actual situation of the questionnaire, the author designed the basic logical idea in the

questionnaire, namely “probe trap” problem, later by screening the two questions, and screen out the effective questionnaire.

(5) Issuing questionnaires. The author generated the questionnaire through the questionnaire star, and distributed the questionnaire through the online social media. After screening out the invalid questionnaire, the valid questionnaire was analyzed and processed.

(6) Data analysis. After receiving the valid questionnaire, after the basic chart analysis of the questionnaire, the author used SPSS to further analyze the correlation and significance of the data, and verified the quality of the questionnaire by checking the reliability.

(7) Research conclusions and reflection. By discussing the analysis results, we speculate the causes behind the results, and combine the analysis results with how to build a good offline shopping platform.

2.literature review

What is privacy? Everyone has a very different understanding of privacy. The discussion of privacy is involved in law, sociology and other disciplines (Chiung-wen (Julia) Hsu, 2006). At the legal level, privacy is vary (Lior Jacob Strahilevitz, 2005). Therefore, in the vast majority of cases, the law is not important to those who infringe. Sociology, however, believes that privacy is determined by the accidental law in the functional differentiation of the social communication system (Katayoun Baghai, 2012). In addition, many scholars have produced different views. For example, privacy is the theory of personal space or area that invades others and invades them (Herman T. Tavani, 2007). Privacy is your “right to be alone” (Warren and Brandeis, 1890). Privacy is the “reservation” (Westin, 1968) and so on. As a result, there has not been a unified concept of privacy.

However, with the advent of the Internet era, the amount of information suddenly increased and people’s information communication became more frequent. The attention to personal privacy has also become an increasing topic of discussion. Many people consider it necessary to sacrifice their privacy for the convenience of living in the Internet age (Gandy, 1993). Therefore, it can be considered that in the Internet era, due to people’s different understanding of information and the diversification of information presentation methods, people’s attention to privacy in the Internet era is different from the privacy in the traditional sense (Kim Bartel Sheehan, 2002). Alan Westin Under the theoretical system based on traditional privacy concerns, people’s concerns about privacy in the Internet era are divided into three categories (FTC, 1996). One is the behavior that affects their privacy in the Internet age, the other is not concerned about it, and the last one depends on the circumstances. In this study, the difference factors of people’s attention to privacy are respectively explained through four aspects: personal belief, attitude, behavior intention and actual behavior.

2.1Personal Beliefs

In terms of personal beliefs, Tamara Dinev concerns that there will be some differences in personal beliefs about government monitoring. Some people think that the government needs more opportunities to obtain relevant information, while some people are worried about government monitoring (Tamara Dinev, Paul Harta & Michael R. Mullen, 2008). Yuan Li Found that the tendency of personal beliefs on privacy has a positive impact on both online privacy concerns and website privacy concerns, and focusing on website privacy concerns is an important indicator to predict the personal disclosure of relevant personal information on the Internet (YuanLi, 2014).

2.2 Attitude

On the level of privacy attitudes, Prashanth Rajiva found that discussions to protect privacy raised concerns when choosing mobile apps (Prashanth Rajivan & Jean Camp, 2016). Govani In users’ attitudes towards Facebook services and privacy settings, it is found that even though people understand Facebook-related privacy issues and available privacy settings, most users have not changed their attitudes towards Facebook (Govani & Pashley, 2005).

2.3 Behavioral intention

In the behavioral intention about privacy, the Hongwei Yang online survey of American college students shows that those whose privacy is somehow violated on the Internet will enhance their intention to forge personal information or refuse to provide personal information (Hongwei Yang, 2012). However, in the research on the privacy concerns of chatbots and mobile advertising, it is found that people’s attitude towards mobile advertising does not directly affect the behavior intention of using chatbots, which is determined by people’s attitude towards chatbots (Lucrezia Maria de Cosmo, Luigi Piper & Arianna Di Vittorio, 2021).

2.4 Actual behavior

In the study of people&#039;s privacy preferences and actual behavior of shopping robots, it is found that even if they pay attention to their privacy in the communication of shopping robots, they will not take practical action (Sarah Spiekermann, Jens Grossklags &amp; Bettina Berendt, 2001). In addition, other studies have found that even if people know the importance of privacy, when they start to interact online, they often ignore their privacy and do not regulate their actual behavior (Bettina Berendt, Oliver Gunther &amp; Sarah Spiekermann, 2005).

Today, the concept of risk tolerance, used in business, has gradually been introduced as a perspective to measure individual attitudes towards privacy. Hallahan T et al. believe that the evaluation criteria of privacy leakage tolerance are similar to the risk tolerance (Hallahan T.A, Faff R.W &amp; Mckenzie M.D, 2004), and that the measurement in the form of questionnaire scale is completely effective. Liang used risk tolerance in information behavior research (Liang H &amp; Xue Y, 2009), which found that users&#039; tolerance of information security risks and their perception of information threat had negative effects. Taken together the results suggest that the applicability of the questionnaire scale of tolerance for relevant measures of privacy attitudes.

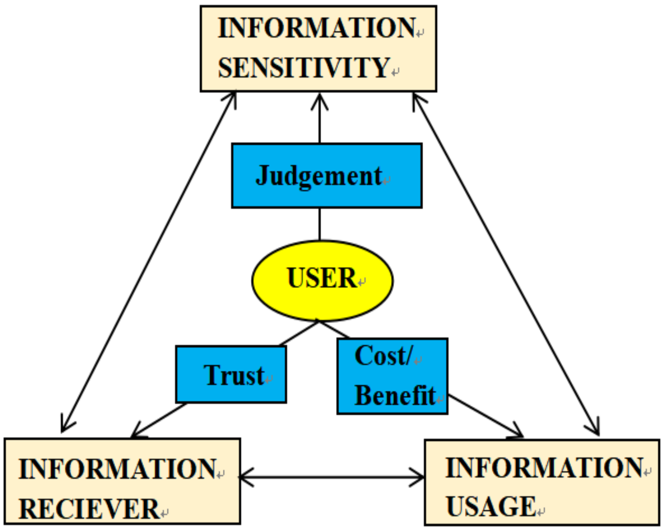
3.Theoretical principle

3.1 Theoretical framework

In fact, as early as the beginning of the 21st century, Adamas, Berrotti, Davis and other scholars have explored and studied the privacy protection under the background of multimedia communication, while Admas has proposed a specific privacy model based on multimedia communication. She points out that the core concept of the privacy model is that the plot of privacy invasion and privacy invasion (the conceptualization of the descriptive narrative of privacy invasion) is actually a privacy invasion cycle. When most privacy violations occur when the user is aware of them, the user’s cognition and the reality are not matched and not coordinated.

Based on the above core views, Admas proposed a privacy model framework from the perspective of three privacy factors, namely, information sensitivity (ISS), receiver sensitivity (ICS) and use sensitivity (IUS). These three factors interact to make users form their overall perception of privacy. Therefore, in different research backgrounds, the relationship of the three factors is specific, and researchers need to weigh these factors and make some assumptions appropriately, such as assuming that users can accept some privacy risks. Then the specific privacy framework is shown in Figure 1 below:

Figure 1 The Adams privacy model framework



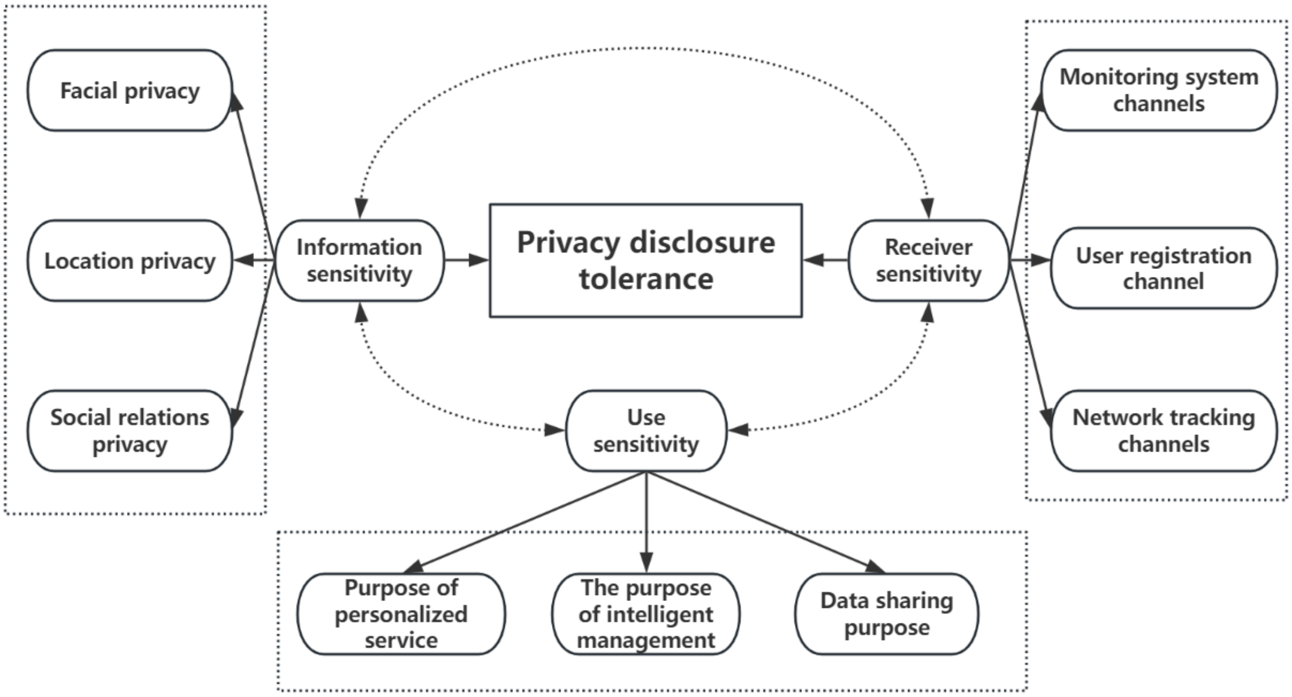
3.2 Study model

With the continuous popularization and application of Adams’ theoretical framework on multimedia privacy in the field of privacy research, Li Rui and other scholars proposed a research model based on Admas theoretical framework in their own related privacy research papers. For example, Li Rui introduced his own model in the empirical investigation of the tolerance of privacy leakage of big data in libraries. The model framework is determined from three aspects: information sensitivity (ISS), receiver sensitivity (ICS), and the use of sensitivity (IUS). Li Rui regards these three aspects as three dimensions, and then in the dimension perspective, he designed the research structure model of "second order, third factors, first order and 12 factors" for the tolerance of library big data privacy leakage.

The author's privacy leakage tolerance investigation model for the offline retail scene is based on the library big data model proposed by Li Rui, and designed as a model specifically for the offline retail scene. The author also starts from the three dimensions of information sensitivity (ISS), receiver sensitivity (ICS) and use sensitivity (IUS), and each specific dimension is subdivided into three indicators. Information type sensitivity refers to the perception and judgment of individual sensitivity to different types of information, which is used to define the content and type of personal privacy that the user allows to disclose; the information reception sensitivity refers to the perception of individual sensitivity to the information collection channel and the tolerance of the information collection channel and method; the information sensitivity refers to the perception of the individual's sensitivity to how the privacy and the acceptable purpose, scope and degree of the use of personal privacy information.

In this way, the author generates the privacy leakage tolerance investigation model of offline retail scenarios with exclusive "second order and third dimension, first order and ninth index". The model diagram is shown in Figure 2 below:

Figure 2 Research model of offline retail scenario


Facial privacy
Location privacy
Social relations privacy
Information sensitivity
Privacy disclosure tolerance
Receiver sensitivity
Monitoring system channels
User registration channel
Network tracking channels
Use sensitivity
Purpose of personalized service
The purpose of intelligent management
Data sharing purpose

After clarifying the theoretical framework and research model of the author's research, the nine questions in the model are subdivided into four questions for each index, and the specific privacy leakage tolerance questionnaire question is designed.

3.3 Variables and scales

For the questionnaire design, the relevant scales must be needed as the support of the questionnaire design. Therefore, starting from the research model, the author designs the corresponding questionnaire questions under the nine indicators to form the questionnaire measurement scale. As a questionnaire variable, in the first part, the variables were the demographic indicators. That is, the gender, age, education level and occupation of the respondent. The second part is based on nine indicators under three dimensions, including facial privacy (FP) under information sensitivity (ISS), Location privacy (LP), Social relations privacy（SP）; monitoring system channel (MSC) under receiver sensitivity (ICS), user registration channel (URC), network tracking channel (NTC); personalized service purpose (PSP) under using sensitivity (IUS), intelligent management purpose (IMP), and data sharing purpose (DSP). The specific scale is shown in Table 1 below：

Table 1 Privacy leakage tolerance questionnaire scale in offline retail scenarios

Research topic	Second order	First order	Measure the project	Contents of a project
Research on the tolerance of consumer privacy leakage in the offline retail shopping scenario	Information-type sensitivity(ISS)	facial privacy (FP)	FP1	I can accept the offline retail stores to take my avatar
			FP2	I can accept the offline retail store records and analyze my facial information
			FP3	I can accept offline retail stores disclosing my facial features
		Location privacy (LP)	LP1	I think the offline retail store can record my visits
			LP2	I can tolerate offline retail stores leaking the areas I often to in the store
			LP3	I can accept offline retail stores storing my phone or WeChat ID
		Social relations privacy(SP)	SP1	I can accept offline retail store users to know my family staff when registering
			SP2	I can tolerate offline retail stores leaking my personal real social relationship information
			SP3	I can accept the offline retail stores to browse and analyze my online friends circle
	under receiver sensitivity(ICS)	monitoring system channel (MSC)	MSC1	I can accept the installation of multiple monitoring devices in the offline retail stores
			MSC2	I can accept recording and viewing my activity in the offline retail store
			MSC3	I can tolerate offline retail stores to monitor my shopping behavior through access control sensing devices
		user registration channel (URC)	URC1	I can accept offline retail stores to collect personal information through user registration
			URC2	I can accept offline retail stores to analyze user registration information for certain purposes
			URC3	I can accept the offline retail stores to disclose my registration information
		network tracking channel (NTC)	NTC1	I can accept the offline retail stores to collect my online browsing information through the background
			NTC2	I can accept the offline retail stores to get the purchase records of my online purchases
	under using sensitivity (IUS)	personalized service purpose (PSP)	PSP1	I can accept offline retail stores to analyze my browsing records to develop personalized product recommendation services
			PSP2	I can tolerate offline retail stores sending messages through wechat official accounts or SMS in order to achieve personalized services
		intelligent management purpose (IMP)	IMP1	I can accept offline retail stores to store and analyze consumers' personal shopping information to realize intelligent management
			IMP2	I can accept offline retail stores to improve their shopping efficiency by monitoring consumer activities
			IMP3	I can tolerate offline retail stores to disclose consumers' personal information for the sake of daily business convenience
		data sharing purpose (DSP)	DSP1	I can accept offline retail stores sharing each other's consumer purchase records or purchase habits
			DSP2	I can accept offline retail stores to provide consumer information to third parties such as database providers for free or for compensation
			DSP3	I can accept offline retail stores to analyze and publish consumer information for product promotion

4.Data analysis

This section mainly describes the process of issuing the questionnaire, the planning and interpretation of the sample, and presents the results of demographic variables; and checks the reliability of the scale, which objectively evaluates the scale reliability by calculating Cronbach&#039;s Alpha. In terms of results, the scale has good reliability; and according to the situation, the data content obtained through the questionnaire generated by the scale can be returned to the research topic of &quot;privacy leakage tolerance survey in offline retail shopping scenarios&quot; and suitable for the measurement of privacy leakage tolerance in the topic.

4.1 Data collection and preprocessing

4.1.1 data collection

This analysis mainly adopts the way of network questionnaire data collection, mainly through the Internet social media tools to obtain convenient samples, such as QQ space, WeChat circle of friends and weibo and other social media tools on the questionnaire, relative to the traditional network questionnaire, through the Internet social media tools to collect data in sample randomness and sample source range has certain limitations, but through the channels of questionnaire collection due to social

The addition of the lines, It has relatively obvious advantages in terms of collection rate; And also retains the basic advantages of the network questionnaire survey —— objective voluntary and anonymous protection; As the questionnaire was delivered through the social media, Therefore, the participants filled out the questionnaire based on voluntary reasons, There is no coercion or other reasons; Secondly, according to the relevant theory of the anonymous effect of P. C. Zimberdo, an American psychologist, When measured by the online questionnaire, As the subjects were in an anonymous state, In an “anonymous uniform,” Can make the individual independence, autonomy is fully reflected, Therefore, the participants’ views and attitudes are more similar to the real attitudes, The results avoid the interference of other external pressure or factors, Make the results more objective.

Due to time problem, the duration of the questionnaire survey from May 23,2021,17 points to May 25,2021,17, lasted 3 days, a total of 237 questionnaires, the overall collection efficiency is higher, it also thanks to the author using public social media tools to questionnaires, in social relations and social expectations, in social group people more active and voluntary fill in the questionnaire, and even willing to help further forward and share, sample size can snowball rapidly, so as to achieve the expectations of the sample size.

4.2.2 data preprocessing

Although the total amount recovered reached the author’s expectation, the author excluded 57 invalid questionnaires after questionnaire screening, and the final number of questionnaires was 180. In addition to the obvious perfunctory filling in, the most important basis is the “probe” problem designed by the author in the questionnaire. At the beginning of the questionnaire design, the author considered the possibility that the questionnaire was filled due to the lack of patience. Therefore, in order to test whether everyone was “consistent” and “not changing the original intention”, the author set questions 23 and 32 of the questionnaire to test the probe. The 23rd question of the questionnaire is “ I can accept the offline retail stores to analyze my browsing records to (AI technology) to carry out personalized product recommendation service.”, And the 32nd question of the questionnaire is” I can accept merchants through my past browsing records to use AI technology to provide personalized services such as product customization and product recommendation.”, It can be seen from the above statement that the two problems are actually expressing the same meaning, so for the subjects, the attitude towards the problem based on the same scenario should be the same or the gap is not large. The scale adopted by the author is 7-point Likert scale, so the author believes that if the difference between the measurement conclusion of the above two questions is greater than 2 points, then the author thinks that the questionnaire is invalid or low-quality questionnaire and should be excluded. Therefore, according to 180 valid questionnaires, the author described and analyzed the sample attributes of demographic variables, as shown in Table 2 below:

Table 2 Sample attribute distribution table

Survey indicators		Quantity	Frequency (%)
Gender	man	92	51.1
	woman	88	48.9
Age	Under the age of 18	7	3.9
	18-24 Years old	117	65.0
	25-34 Years old	38	21.1
	35-44 Years old	4	2.2
	Over 45 years old	14	7.8
Education level	High school and below	11	6.1
	junior college education	20	11.1
	undergraduate course	93	51.7
	Master / doctor	56	31.1
Occupation	Personnel of state government organs and public institutions	23	12.8
	Doctors, teachers and other professional technicians	18	10.0
	Private sector or self-employed labor company employees	45	25.0
	Business and services industry personnel	12	6.7
	soldier	2	1.1
	student	80	44.4
Monthly income	Below 3K	77	42.8
	3K-5K	35	19.4
	5K-8K	28	15.6
	8K-12K	21	11.7
	More than 12K	19	10.6

From table 2, the ratio of men and women to close to 1:1, basic, and the questionnaire subjects 86.1% is from 18-24 or 25-34 young adults, and the part is the mainstay of the current social line retail store consumer population today, so the distribution of the sample has certain representative, accord with the research needs and subject content.

4.2Scale reliability check

In the above according to the relevant research model and theory form belongs to the author research topic research scale, the author also want to check and judge the indicators of the scale (item) can fit in the research topic, in other words, also hope that through reliability check to see if the questionnaire topic can accurately measure to the author wants to measure the variables. Therefore, the reliability check method is to observe the α -value size of Cronbach's Alpha to conduct the reliability evaluation. Clone Bach coefficient is a commonly used reliability evaluation index in the social science research field, which overcomes the disadvantage of partial halving and measures the internal consistency of the scale by calculating the coefficient (α value); the larger α value, the higher the scale; since the deleted α value can be obtained by SPSS software, the author can update the scale according to the change of α value to improve the credibility of the scale.As shown in Table 3 below.

Table 3 reliability adjusted scale

Second order	**First order**	**Measure the project**	**The correction was total correlated**	**α price**
Information-type sensitivity(ISS)	facial privacy (FP)	FP1	0.678	0.816
		FP2	0.817	
		FP3	0.613	
	Location privacy (LP)	LP1	0.519	0.678
		LP2	0.480	
		LP3	0.516	
	Social relations privacy(SP)	SP1	0.866	0.917
		SP2	0.848	
		SP3	0.822	
under receiver sensitivity(ICS)	monitoring system channel (MSC)	MSC1	0.681	0.862
		MSC2	0.770	
		MSC3	0.770	
	user registration channel (URC)	URC1	0.657	0.764
		URC2	0.716	
		URC3	0.515	
	network tracking channel (NTC)	NTC1	0.738	0.843
		NTC2	0.738	
under using sensitivity (IUS)	personalized service purpose (PSP)	0.672		0.804
	intelligent management purpose (IMP)	0.672		
	data sharing purpose (DSP)	0.745		0.813
Information-type sensitivity(ISS)	facial privacy (FP)	IMP3	0.788	
		IMP2	0.526	
	Location privacy (LP)	DSP1	0.658	0.860
		DSP2	0.833	
		DSP3	0.737	

As can be seen from Table 3, the total correction correlation of each measurement item of the scale is above 0.5, and the clonal Bach coefficient (α value) can reach about 0.8 in the second order dimension, and the general standard of social science research (α value above 0.7).

4.3 Data presentation

After the scale reliability test, the issuance and recovery of questionnaires, and the data pretreatment, The author presents the mean value and standard deviation of each dimension and index through SPSS software, We hope to find out the causes and practical significance behind it through data comparison, And outside of the scale, Measurement questions of consumer "behavioral variables" were added at the end of the questionnaire, And Pearson correlation between the behavioral variables and the dimensions, Observed with a significant positive correlation, The specific data contents are shown in Tables 4 and and 5 below, The analysis of the outliers observed in the data and the causes and practical significance will be further discussed in the subsequent subsections.

Table 4 Mean value, standard deviation

Second order	First order	Measure the project	Mean value	Standard deviation
ISS (1.89)	FP (1.88)	FP1	2.36	1.806
		FP2	1.87	1.364
		FP3	1.41	1.066
	LP (2.36)	LP1	3.04	2.065
		LP2	1.69	1.309
		LP3	2.37	1.560
	SP (1.42)	SP1	1.45	1.032
		SP2	1.29	0.887
		SP3	1.52	1.179
ICS (2.23)	MSC (2.87)	MSC1	3.61	2.155
		MSC2	2.25	1.880
		MSC3	2.76	1.962
	URC (1.96)	URC1	2.28	1.607
		URC2	2.24	1.623
		URC3	1.37	0.933
	NTC (1.86)	NTC1	1.71	1.331
		NTC2	2.00	1.575
IUS(2.17)	PSP (2.56)	PSP1	2.53	1.804
		PSP2	2.58	1.756
	IMP (2.27)	IMP1	2.71	1.844
		IMP2	2.52	1.735
		IMP3	1.58	1.228
	DSP (1.69)	DSP1	1.91	1.462
		DSP2	1.53	1.207
		DSP3	1.62	1.283

Table 5 Correlation measures of the behavioral variables

Second order	First order	Behavioral variables
ISS	FP	0.496**
	LP	0.600**
	SP	0.371**
ICS	MSC	0.645**
	URC	0.633**
	NTC	0.537**
IUS	PSP	0.612**
	IMP	0.647**
	DSP	0.508**

5.Results of discussion and reflection

5.1 Results for discussion

According to the overall analysis results, the author shows that consumers 'tolerance of privacy leakage in offline retail scenes is relatively low. In fact, this is also in line with the phenomenon that people pay more attention to personal information privacy in today's society, which is within the expected range of the author. According to the figure above, the average value of the data is basically below 3 (disagree) in terms of dimension (ISS, ICS, IUS) or specific indicators (respectively), which shows that the overall attitude is a negative attitude.

From the ISS dimension, consumer tolerance for different information types are collected from low to high for social relations privacy, facial privacy, location privacy, and the gap between the indicators span is larger, so I know that consumers in offline shopping, for location privacy tolerance than other types of information, of course it also exists because the author of the preset scene itself is based on the "offline".

In terms of ICS dimension, the overall data of this dimension is higher than that measured in the other two dimensions, that is, compared with what channel the information is obtained, consumers are more concerned about what information it is obtained and how it is used by merchants. ICS dimension monitoring system channel (MSC) has a high mean in the questionnaire, find the reason, because consumers for indicators "receive offline installation monitoring system" high tolerance, also for businesses using the monitoring system record behavior tolerance is higher, it also shows that consumers can actually stand in the position of the businessman, in order to prevent theft or other reasons, even if may cause privacy, but due to certain legitimacy, also tolerate merchants put cameras for information.

In the measurement of the IUS dimension, very interesting phenomena are found. There are certain "double standards" for consumers about the use of information. Since the author adopts the method of seven measures, and the overall measurement is within 3, the author believes that in the data recovered this time, the mean value greater than 2.5 can be regarded as high, while the degree of about 1.5 is low. In IUS, from the above perspective, it can be found that the index PSP1.PSP2.IMP1. IMP2. has an obvious gap with IMP3.DSP2.DSP3; through reviewing the problems, it is not difficult to find that the use method with high consumer tolerance is nothing more than "personalized recommendation, improving shopping efficiency and intelligent management", and if the merchants use the information for sharing and analysis, the attitude of consumers will plummet. It also proves that consumers for privacy information use "double standard", consumers are willing to sacrifice some privacy information to improve their shopping experience and convenient degree, but not willing to merchants for merchants own sharing and management, embodies the "information collected from me this can only be used to serve me, not for" conservative attitude.

In addition, in addition to measuring the tolerance of consumer privacy leakage, in order to get more enlightenment, the author designed the question of consumer behavior variables in the questionnaire in addition to the scale. Consumers are open to shopping after obtaining personal information, and the author also tries to ask some of the subjects

5.2 Reflection

Through the analysis of the above results, it is not difficult to find that consumers now have a negative attitude towards offline retail stores to obtain personal information, but it is not irrational "brainless unwilling", just as the consumers have the tolerance of "monitoring system acquisition" generally, consumers sometimes think from the perspective of the business; from the perspective of beneficial or beneficial, so they are willing to sacrifice some personal information for greater benefit. Therefore, we can have the following reflections on how to build a good offline shopping environment.

5.2.1 For the consumers

(1) Improve consumers' tolerance for information acquisition. From the conclusion, the author learned that consumers' aversion to the monitoring system channel is not so strong, and they can obtain information through the monitoring system channel, and the author studied the original Background The "Wandian Palm" incident is also the use of AI camera to capture information, but it is still necessary to inform consumers in advance, so that consumers can feel respected and have the right to independent choice, so as to improve the perception of consumers.

(2) Let consumers feel that they have gained their dividends after collecting their own information, which will greatly improve the shopping experience. For example, consumers can only recommend and customize customized services, so that consumers can feel that their information is "profitable" after it is obtained, so that consumers will gradually relax the control of their own information, forming a virtuous cycle.

5.2.2 For businesses

In order to build a good shopping environment, merchants also want to do, remove the optimization, more is in the aspect of information use can have good norms, wanton use shall not be allowed and leak, according to the study, consumers most hate information use is personal information in the way to paid or free, so if businesses can do consumer personal information protection, consumers to have trust for merchants, thus forming merchants can obtain profits, consumers can enjoy more quality service of good cycle, help each other to build a good offline shopping environment.

Funding

no

Conflict of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Reference

[1] Baghai, K. (2012). Privacy as a human right: A sociological theory. Sociology, 46(5), 951-965.

[2] Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. Communications of the ACM, 48(4), 101-106.

[3] Brandeis, L., & Warren, S. (1890). The right to privacy. Harvard Law Review, 4(5), 193-220.

[4] de Cosmo, L. M., Piper, L., & Di Vittorio, A. (2021). The role of attitude toward chatbots and privacy concern on the relationship between attitude toward mobile advertising and behavioral intent to use chatbots. Italian Journal of Marketing, 1-20.

[5] Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. The Journal of Strategic Information Systems, 17(3), 214-233.

[6] Federal Trade Commission. (1996). Consumer information privacy hearings [online]. http://www.ftc.gov

[7] Gandy Jr, O. H. (1993). African Americans and privacy: Understanding the black perspective in the emerging policy debate. Journal of Black Studies, 24(2), 178-195.

[8] Govani, T., & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. Privacy Policy, Law, and Technology Course. Carnegie Mellon University.

[9] Hallahan, T. A., Faff, R. W., & McKenzie, M. D. (2004). An empirical investigation of personal financial risk tolerance.

Financial Services Review, 13(1), 57-78.

[10] Hsu, C. W. J. (2006). Privacy concerns, privacy practices and web site categories: Toward a situational paradigm. Online Information Review.

[11] Li, Y. (2014). A multi-level model of individual information privacy beliefs. Electronic Commerce Research and Applications, 13(1), 32-44.

[12] Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly, 71-90.

[13] Rajivan, P., & Camp, J. (2016). Influence of privacy attitude and privacy cue framing on android app choices. In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016).

[14] Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. The Information Society, 18(1), 21-32.

[15] Spiekermann, S., Grossklags, J., & Berendt, B. (2001, October). E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. In Proceedings of the 3rd ACM conference on Electronic Commerce (pp. 38-47).

[16] Strahilevitz, L. J. (2005). A social networks theory of privacy. The University of Chicago Law Review, 919-988.

[17] Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. Metaphilosophy, 38(1), 1-22.

[18] Westin, A. F. (1968). Privacy and freedom. Washington and Lee Law Review, 25(1), 166.

[19] Yang, H. (2012). Young American consumers' prior negative experience of online disclosure, online privacy concerns, and privacy protection behavioral intent. Journal of Consumer Satisfaction, Dissatisfaction & Complaining Behavior, 25, 179-202.