The Moderation Role of Trust in the Privacy Paradox of Online Shopping Platforms

Yukai Hao*, Liangxi Wang

Corresponding author: haoyukai@163.com*, 1849055151@qq.com

School of Management, Wuhan University of Technology, 122 Luoshi Road, Hongshan District, Wuhan, China

Abstract. Starting from the discovery of the phenomenon of privacy paradox and several explanations of privacy paradox, this paper explores the privacy paradox in the context of online shopping through the questionnaire method. The results show that the privacy paradox also exists in the online shopping context and that trust plays a moderating role in the privacy paradox. In addition, this paper discusses the impact of information security technology and related policies and regulations on trust, and thus provides some suggestions for online shopping platform enterprises.

Keywords: privacy paradox; trust; privacy calculus

1 Introduction

Online shopping is a kind of shopping method in the ascendant, and the online shopping economy has gradually become an important pillar in China's economy. As of June 2022, the scale of online shopping users in China reached 841 million, accounting for 80% of the total number of Chinese netizens^[1]; it was reported that the sales on the Double 11 day in 2021 reached 540.3 billion yuan, and on the other hand, the total online retail sales of physical commodities in the first half of 2022 reached 5.45 trillion yuan, accounting for 25.9% of the total retail sales of consumer goods in the society. These data show that online shopping has become a common shopping method for consumers, and the online shopping economy has become an important part of China's economy.

While online shopping breaks the constraints of time and space and enables retailers to reach new markets and new consumers, retaining them and earning their long-term trust and loyalty has become a challenge, especially when protecting consumer privacy has become a key barrier to e-commerce development^[2]. Online shopping platforms rely on consumers' own information to push products to them, and consumers' concern for their privacy is gradually increasing in China. According to Penguin Intelligence's 2018 Chinese Netizen Privacy Status Survey Report, netizens have concerns when filling out their personal information, but at the same time, only 14% of netizens defend their rights when they find their information has been leaked, and this inconsistency between attitudes and behaviors towards privacy is known as the privacy paradox.

The privacy paradox in the context of online shopping can be understood as the fact that although consumers provide personal information to online shopping platforms relatively easily, it does not mean that consumers have full trust in the online shopping platforms. In order for online shopping platforms to gain consumers' trust and loyalty, and to realize long-term sound development, this paper studies the phenomenon of privacy paradox in online shopping platforms and tries to provide suggestions for online shopping platform enterprises.

There are two main areas of current research on the privacy paradox:

First, whether there is a privacy paradox. The phenomenon of privacy paradox was discovered by Brown in 2001, and the concept of privacy paradox was introduced by Barnes in 2006 to describe the phenomenon of consumers' increased concern about the risk of privacy breaches on the Internet and their indifference in implementing measures to protect their privacy^[3]. Since then a number of studies have argued for the existence of the consumer privacy paradox phenomenon in the Internet. These studies have focused on the aspect of social software, and the field of this paper is online shopping platform, so it is necessary to argue the existence of privacy paradox in online shopping platform first.

Second, how to explain the privacy paradox. After discovering the phenomenon of privacy paradox, many scholars have tried to explain it. It is more common to explain the privacy paradox phenomenon with privacy computation theory, heuristic theory or coping behavior theory, but there has not yet appeared an academically recognized theory that can explain the privacy paradox. This paper tries to propose a model based on the APCO frame and using trust as a moderating variable, which is used to explore the two questions of whether there is a privacy paradox phenomenon and how to explain the privacy paradox in the context of online shopping.

2 Literature Review

2.1 Privacy Paradox

Discussion of the privacy paradox first appeared in 2001 by Brown, who found that despite expressing concerns and worries about their privacy, people were willing to give out their personal information if the rewards were sufficient.In 2006, Barnes studied the behavior of teens on social networks and found that despite teens expressing concerns about their privacy (questionnaire results showed that most of the teens did not believe that "everyone should know everything about everyone else"), they still freely shared their personal information on social networks. He called this phenomenon the privacy paradox. Since then, the privacy paradox has aroused the interest of scholars for a long time, and many scholars have conducted empirical research and analyzed the causes of the privacy paradox.

The explanation given by Barnes in his paper for the cause of the privacy paradox was that adolescents confused the boundaries between cyberspace and private space, believing that their information would not be seen by their parents or other institutions, when in fact cyberspace is a public space and the personal information they disclose can be utilized in ways they did not expect. Other scholars have also given their own explanations for this phenomenon.

Debatin illustrated through the questionnaire survey method combined with experiments that the actual attitude towards privacy diffusion shown by users is caused by high satisfaction with social network platforms, usage habits and the third-person effect. That is to say, users are highly satisfied with the experience brought by social networking platforms and are accustomed to using them in their daily lives, on the other hand, users believe that the risk of privacy leakage is more likely to happen to other people than to themselves, and these reasons lead to the diffuse attitude of users in disclosing their personal information on social networks^[4]. Christofides recruited 343 students who use Facebook as volunteers to study the relationship between information disclosure, information control, and personalities. The study found that there was not a very significant negative correlation between disclosure and information control, meaning that disclosure and information control may not be opposite ends of the spectrum, and that focusing on control of information does not necessarily mean less disclosure. Follow-up studies have shown that the degree of disclosure appears to be significantly correlated only with the need to be popular, whereas the degree of information control is related to self-esteem and trust. Thus, Christofides suggests that the reason people express concerns about privacy yet proactively disclose personal information is that people want to construct their personal identity in cyberspace by disclosing more personal information and, as a result, gain more popularity^[5]. Christofides' conclusion is known as the social needs theory, which states that the privacy paradox arises primarily from people's need to value themselves socially. In addition, other scholars have attempted to explain the privacy paradox using the theory of utility maximization in economics. Awad argues that in each case, individual behavior related to the use of a particular technology is guided by the maximization of total utility^[6]. The privacy calculus theory holds that people always consider the perceived risks and perceived benefits brought by privacy disclosure before making privacy disclosure decisions. Tang used privacy calculus theory to study the reasons why people disclose false information in social apps, and gave some suggestions^[7]. This paper will also study the privacy paradox in the field of online shopping platform based on the privacy calculus theory and APCO framework.

2.2 Privacy Calculus Theory

The term privacy calculus theory is derived from the calculus of human behavior. Privacy calculus theory holds that people will rationally weigh the risks and benefits of privacy disclosure when making privacy disclosure decisions. Privacy calculus theory is often combined with expectation theory, which states that people maximize expected benefits and minimize expected risks.

The two most important metrics in privacy calculus theory are privacy risk and perceived benefit. Privacy risk refers to people's fear that their information will be improperly used by organizations^[8], such as being sold to third parties or used in user portraits, etc. These risks lead to people's concern about privacy. Clearly, privacy concerns reduce people's willingness to disclose information about themselves. In the context of online shopping, this means that privacy concerns will reduce people's willingness to use online shopping platforms. To measure the level of privacy concerns, the IUIPC scale is used. The IUIPC scale measures people's privacy concerns from multiple dimensions such as cognition, collection and control. Compared with other scales, IUIPC scale is more suitable for the Chinese Internet situation [9]. Expected revenue refers to the potential revenue that people can get from disclosing personal information.

In recent years, privacy calculus theory has been widely used in the acceptance research of new technologies. Mengxi Zhu et al. used the privacy calculus theory to explain the privacy paradox in mHealth and proposed that designers of mHealth applications should optimize their interactive functions to increase users' perceived benefits^[10]. By using privacy calculus theory to analyze social apps, Jozani found that people are gradually reducing their participation in social apps because of privacy concerns^[11]. Natalia et al. used privacy algorithmic theory for smart homes and found that the more human-like a smart home is, up to a certain point, the more it increases the perceived benefit to the user, but beyond a certain point, it increases privacy concerns^[12].

As a flourishing shopping method, online shopping has improved the shopping experience of consumers, and the online shopping economy has become an important part of China's economy. Analyzing the phenomenon of privacy paradox in the field of online shopping through privacy algorithm theory is both theoretically reasonable and of practical significance. In this paper, we will analyze the privacy paradox phenomenon in the field of online shopping through privacy algorithm theory, and put forward measures to increase consumers' perceived benefits, expecting to enhance consumers' willingness to buy online and stimulate the growth of online shopping economy at the same time.

3 Model and Hypothesis

This paper deals with the model as shown in Fig.1, and the significance of each variable is described next.



Fig. 1 Model for privacy concern

3.1 Privacy Concern

Privacy concerns in this context refer specifically to consumers' concerns about the possible risks associated with the exposure of their information when using online shopping platforms.

The use of online shopping platforms undoubtedly exposes a lot of personal information, such as addresses, cell phone numbers, shopping habits, and so on. According to the privacy algorithm theory, when using online shopping platforms, consumers will weigh the expected benefits of using online shopping platforms against the perceived privacy risks, i.e., consumers' willingness to use online shopping platforms is affected by privacy concerns. This leads to the first hypothesis:

H₁: Consumers' privacy concerns about platform companies can negatively affect consumers' willingness to use them.

Consumer privacy concerns arise from considerations of fairness in the transaction process. Consumers fear that they are being treated unfairly in transactions in which they provide privacy in exchange for a benefit, and this leads to privacy concerns. With regard to the definition of "fairness," invoking social contract theory, it is argued that a company's collection of personally identifiable data is considered fair only if the consumer is granted control over the information and is informed of the company's intended use of the information. That is, a company's behavior in collecting personally identifiable data (COLLECTION), whether consumers have control over the information (CONTROL), and whether consumers are informed of the company's intended use of the information (AWARENESS) all have an impact on consumers' privacy concerns about platform companies. Based on the above discussion, following three hypotheses are proposed:

H_{2a}: Companies' collection of personally identifiable data raises consumer privacy concerns

H_{2b}: Consumers having control over information reduces consumer privacy concerns

H_{2c}: Consumers being informed of a company's intended use of information reduces consumer privacy concerns

3.2 Trust

Trust in this context refers to the consumer's acceptance of the firm's ability to ensure that his or her privacy is not abused or violated by other individuals or organizations. Many studies have shown that the negative impact of such privacy concerns is moderated by consumers' trust in platform firms. Starting from this aspect of explanatory level theory, Li He et al. experimentally verified that trust moderates the impact of privacy concerns on users' disclosure behavior on social media^[13]. Duan et al. concluded from their study in the context of trajectory tracking applications that trust can significantly reduce the perceived risk of, and thus alleviate, privacy concerns^[14]. This leads to the third hypothesis:

 H_3 : Consumer trust in platform firms reduces the negative impact of privacy concerns on willingness to use.

A user privacy breach at a platform company reduces consumer trust.2022 Four Facebook users have accused Facebook of continuing to track the trajectory of their online activity after they quit the social media network. According to a survey from The Verge, only 41% of users trust Facebook to protect their information. But privacy breaches aren't necessarily the result of corporate surveillance. Marriott shares fell 5.6% on the day the news was revealed that 500 million customers' data was at serious risk of being compromised after the hacking of the Starwood hotel room booking database under Marriott International; and a massive data

breach of MyFitnessPal, the diet and nutrition management app and website of US functional sports brand Under Armour, in which as many as 150 million users' information was stolen. These attacks from the outside can be prevented by upgrading information security technology, which leads to the fourth hypothesis:

H₄: Upgrading information security technology by platform companies can improve consumer trust in platform companies.

On the other hand, the supervision and management of the external environment can also effectively reduce the occurrence of information leakage incidents. So the fifth hypothesis is proposed:

H₅: Improving information security-related policies and regulations can increase consumer trust in platform companies.

3.3 Perceived Benefit

According to privacy algorithm theory, when consumers make privacy decisions, they weigh the benefits and risks associated with the decision, and they make a decision when the benefits associated with the decision outweigh the risks. Consumers' perceived risks can be measured by privacy concerns, and consumers' perceived benefits we measure using perceived ease of use and perceived usefulness in the TAM model. Obviously, the greater the consumer perceived benefit, the greater the consumer's willingness to use. Therefore the sixth hypothesis is proposed:

H₆: Consumers' perceived benefits have a positive effect on consumers' willingness to use.

4 Questionnaire Design and Analysis of Experimental Results

4.1 Sample selection and data analysis

This paper adopts the questionnaire survey method to obtain the attitude of users who use online shopping platforms towards their privacy. The questions in the questionnaire are all derived from authoritative questionnaires such as IUIPC, and are modified for this paper after combining with practical application scenarios. The questionnaire utilizes a five-point Likert scale, where "1" means "strongly disagree" and "5" means "strongly agree".

In this paper, unreasonable questionnaires are excluded according to the following criteria: 1. those whose answer time is less than 1 minute; 2. those whose attitudes are obviously contradictory in the same category; 3. those who answer the same for several consecutive topics. In this survey, a total of 500 questionnaires were distributed and 456 valid questionnaires were obtained, with a validity rate of 91.2%, of which the anthropometric characteristics of the respondents are shown in Table 1.

Table 1 Statistical results of sociological characteristics of the sample

Variable	Category	Percentage (%)	Sample size
CON	male	53.29	243
sex	female	46.71	213
age	Under 18	9.87	45

	18-25	29.39	134
	26-30	39.47	180
	Over 31	21.27	97
	High school and below	14.91	68
	junior college	30.48	139
educational	University		
background	undergraduate	42.76	195
	Master's degree or		
	above	11.84	54

4.2 Analytical Method

In this paper, SPSS was used to analyze the reliability and validity of the questionnaire, and the analysis results are shown in Table 2. The results showed that nine variables, including privacy concerns and perceived benefits, could explain 74.066% of the total variables, while a single variable could not explain all the variables. The homology error of the data was within a reasonable range, and the Kronbach coefficient of each variable was above 0.7, indicating good internal consistency and reliability of the scale. Through the KMO analysis of the questionnaire data, it is found that the KMO values of the questionnaires are all greater than 0.7, so the data can be used for factor analysis. The overall KMO index of the questionnaire is greater than 0.7 and the significance of Bartley sphericity test is much less than 0.05, so the questionnaire can be considered to have good validity.

In addition, regression analysis is used to examine the moderating effect of trust. As can be seen from Table 3, the sig value of the interaction term coefficient is less than 0.05, indicating that there is an adjustment effect.

			•		
Latent Variable	Measured Variable	Item Deleted Cronbach's Coefficient	Overall Cronbach's Coefficient	Cumulative Explanation of Total Variance (%)	КМО
	AW1	0.728			
Awareness	AW2	0.719	0.796	32.265	0.710
	AW3	0.721			
	CT1	0.741			
Control	CT2	0.720	0.811	39.272	0.714
	CT3	0.760			
	CL1	0.777			
Collection	CL2	0.711	0.804	45.156	0.704
	CL3	0.703			
Driveou	PC1	0.754			
Comport	PC2	0.789	0.803	50.525	0.712
Concern	PC3	0.756			
Willing To	WU1	0.744			
Winnig 10	WU2	0.759	0.826	55.731	0.721
Use	WU3	0.748			
Doligios &	PR1	0.744			
Policies &	PR2	0.729	0.816	60.659	0.716
Regulations	PR3	0.766			
security	ST1	0.765	0.836	65.500	0.726

Table 2 Reliability test results

technology	ST2	0.787			
	ST3	0.767			
	TR1	0.775			
Trust	TR2	0.796	0.851	70.035	0.731
	TR3	0.806			
Demosity	PB1	0.700			
Perceiveu	PB2	0.725	0.792	74.066	0.707
Denent	PB3	0.725			

R R² Adjusted SE Change statistic R^2 F Change df1 df2 Sig. F Durbin-V

Table 3 An examination of the moderating effect of trust

Model	R	\mathbb{R}^2	R ²	SE	R ² Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.530ª	.280	.277	.87413	.280	88.260	2	453	.000	
2	.542 ^b	.293	.289	.86710	.013	8.376	1	452	.004	1.875

a. Predictors: (Constant), TR, PC $\,\circ\,$

b. Predictors: (Constant), TR, PC, TRxPC $\,\circ\,$

c. Dependent variable : WU

4.3 Analysis of experimental results

4.3.1 Correlation coefficient matrix

As can be seen from Table 4,5,and 6, in the three groups of relationships, the correlation coefficient between the variables in each group is less than 0.6, indicating that there is no multicollinearity between the variables.

T 11 4	D '	1	1	· · ·	
I Shia /I	Privacy	naradov	correlation	coefficient	matriv
	1 II vac v	Darauon	conciation	COULICICIU	mauin
		L			

	PC	WU	TR	PB
PC	1	-		-
WU	408**	1		
TR	490**	.494**	1	
PB	316**	.342**	.343**	1

**. There was a significant correlation at the.01 level (bilateral)

Table 4 Privacy paradox	correlation	coefficient m	natrix
-------------------------	-------------	---------------	--------

	AW	CT	CL	PC
AW	1			
CT	.395	1		
CL	.339	.365	1	
PC	.345	.323	.381	1

**. There was a significant correlation at the.01 level (bilateral)

Table 5 Trust correlation coefficient matrix	Table 5	Trust	correlation	n coefficient	matrix
--	---------	-------	-------------	---------------	--------

	PR	ST	TR	
PR	1			
ST	.397	1		
TR	.341	.360	1	
deale 1991		1	1 .0.1	_

**. There was a significant correlation at the.01 level (bilateral)

4.3.2 Structural Model

Through the questionnaire, it can be seen that in the context of online shopping, most consumers still choose to use online shopping platforms despite their concerns about their privacy, which proves the existence of privacy paradox in the context of online shopping. Under this premise, we can continue to explore the causes of privacy paradox.

As can be seen from Table 7, consumers' concern about their privacy has a significant negative impact on their intention to use the online shopping platform (β =-0.464, p<0.01). H₁ is established, consumers' concern about their privacy exposure will reduce consumers' willingness to use the online shopping platform. On the other hand, consumers' perceived benefit has a significant positive effect on their intention to use (β =0.282, p<0.01), and H₆ is established. These two data show that consumers are still willing to use online shopping platforms for shopping because the perceived benefits brought by the use of online shopping platforms outweigh consumers' concerns about their privacy exposure. The collection of consumer data by online shopping platforms will cause privacy concerns of consumers (β =0.384, p<0.01), the use of data without consumers' knowledge will also cause privacy concerns of consumers (β =0.285, p<0.01), and consumers will worry about their privacy when they feel that they cannot control their data (β =0.195, P<0.01).

		Estimate	S.E.	C.R.	Р
PC_mean	AW_mean	.285	.063	4.514	***
PC_mean	CT_mean	.195	.059	3.322	***
PC_mean	CL_mean	.384	.068	5.612	***
WU_mean	PB_mean	.282	.061	4.630	***
WU_mean	PC_mean	464	.061	-7.642	***
AW1	AW_mean	1.000			
AW2	AW_mean	1.029	.079	13.033	***
AW3	AW_mean	1.044	.080	13.103	***
CT1	CT_mean	1.000			
CT2	CT_mean	1.038	.074	13.991	***
CT3	CT_mean	.971	.071	13.659	***
CL1	CL_mean	1.000			
CL2	CL_mean	1.121	.085	13.241	***
CL3	CL_mean	1.216	.091	13.334	***
PC1	PC_mean	1.000			
PC2	PC_mean	.934	.060	15.571	***

Table 6 Structure model results

		Estimate	S.E.	C.R.	Р
PC3	PC_mean	1.045	.063	16.551	***
WU1	WU_mean	1.000			
WU2	WU_mean	.955	.063	15.158	***
WU3	WU_mean	1.027	.067	15.318	***
PB1	PB_mean	1.000			
PB2	PB_mean	.961	.075	12.817	***
PB3	PB_mean	.942	.073	12.854	***

As shown in Table 8, the result of path anylysis of this model performed well(CFI>0.9, NFI and TLI are close to 0.9).

Tal	ble 7 Mod	el fit para	ameters		
Model	NFI	RFI	IFI	TLI	CEI
Widder	Delta1	rho1	Delta2	rho2	CFI
Default model	.872	.849	.907	.889	.906
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

As shown in Table 9, in terms of consumers' trust in online shopping platforms, legally compliant policies and regulations as well as complete and reliable security technologies can positively affect consumers' trust (β =0.256, p<0.01; β =0.280, p<0.01).

Table	8	Regression	analysis	on	TR
Table	U	Regression	anarysis	on	111

Model	Nonnormalized coefficient		Standard	4	Sia	
	В	SE	coefficient	ι	Sig.	
	(Constant)	1.197	.186		6.442	.000
1	PR	.256	.051	.235	5.060	.000
	ST	.280	.049	.267	5.753	.000

a. Dependent variable: TR

5 Discussion

5.1 Discussion of experimental results

First of all, through questionnaire survey, this paper confirms that privacy paradox also exists in the context of online shopping, that is, on the one hand, consumers are worried that their privacy may be exposed in the process of using online shopping platforms, on the other hand, they still use online shopping platforms. This phenomenon can be explained by the privacy calculus theory, privacy concerns negatively affect consumers' intention to use, and perceived benefits positively affect consumers' intention to use. When consumers' perceived benefits exceed consumers' privacy concerns, consumers will make use decisions. In this process, trust acts as a moderating variable, diminishing the impact of consumer privacy concerns. When consumers trust online shopping platforms, the negative impact of privacy concerns is lessened. In addition, improved policies and regulations as well as cutting-edge information security technologies can affect consumers' trust in online shopping platforms. When policies and regulations are perfect, consumers believe that their interests are protected by law, and the risk of privacy disclosure will be reduced. When the platform adopts cutting-edge information security technology for information protection, consumers believe that their privacy is difficult to leak.

5.2 Conclusion

Based on the privacy calculus theory and adding trust as a moderating variable, this paper constructs a privacy paradox model in the context of online shopping, and verifies the existence of privacy paradox in the context of online shopping. On this basis, through in-depth exploration of consumers' privacy concerns and trust, three factors affecting consumers' privacy concerns on online shopping platforms are found, namely, the platform's collection of consumer information, consumers' control of their own information, and consumers' knowledge of their own information processing, as well as two factors affecting consumers' trust in online shopping platforms. That is, laws and regulations related to privacy protection and information security technologies adopted by online shopping platform enterprises. The collection of consumer information, or the use of their information without their knowledge will increase consumers' privacy concerns, while perfect policies and regulations and cutting-edge information security technologies can increase consumers' trust in online shopping platform enterprises.

Based on the above conclusions, the followll as industry regulations can help companies gain the trust of consumers.

References

[1] CNNIC releases 49th Statistical Report on the Development Status of China's Internet [J]. News Wave,2022,(2): 3

[2] Eduard Cristóbal Fransi; Frederic Marimon Viadiu. A study of e-retailing management: analysing the expectations and perceptions of Spanish consumers[J].International Journal of Consumer Studies,2007,Vol.31(6): 613-622

[3] Susan B. Barnes.A Privacy Paradox: Social Networking in the United States[J].First Monday,2006,Vol.11(9)

[4] Debatin, Bernhard,Lovejoy, Jennette P,Horn, Ann-Kathrin,et al. Facebook and online privacy: Attitudes, behaviors, and unintended consequences.[J].Journal of Computer-Mediated Communication,2009,Vol.15(1): 83-108

[5] Emily Christofides; Amy Muise; Serge Desmarais; Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? [J]. CyberPsychology & Behavior, 2009, Vol. 12(3): 341-345

[6] Naveen Farag Awad and M. S. Krishnan. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization[J]. MIS Quarterly, 2006, Vol. 30(1): 13-28

[7] Jie Tang;Bin Zhang;Shuochen Xiao.Examining the Intention of Authorization via Apps: Personality Traits and Expanded Privacy Calculus Perspectives[J].Behavioral Sciences,2022,Vol.12(7): 218

[8] Adrija Majumdar;Indranil Bose.Privacy Calculus Theory and Its Applicability for Emerging Technologies[J].E-Life: Web-Enabled Convergence of Commerce, Work, and Social Life,2016,Vol.258: 191-195

[9] Yang Shu, Wang Yuan, Wang Kanliang. Research on privacy Concern Scale suitable for Chinese consumers in Internet environment [J]. Information Journal,2008,(10): 3-7

[10] Mengxi Zhu;Chuanhui Wu;Shijing Huang;Kai Zheng;Sean D. Young;Xianglin Yan;Qinjian Yuan.Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue[J].Telematics and Informatics,2021,Vol.61: 101601

[11] Jozani, Mohsen; Ayaburi, Emmanuel; Ko, Myung; Choo, Kim-Kwang Raymond. Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective.[J].Computers in Human Behavior,2020,Vol.107: 106260

[12] Lavado-Nalvaiz, Natalia;Lucia-Palacios, Laura;Pérez-López, Raúl.The role of the humanisation of smart home speakers in the personalisation–privacy paradox.[J].Electronic Commerce Research & Applications,2022,Vol.53

[13] Li He, Yu Lu, Xu Yiming, Xie Mengfan. A study of social network privacy paradox from the perspective of explanation level theory[J]. Journal of Intelligence,2018,Vol.37(1): 1-13

[14] Sophia Xiaoxia Duan;Hepu Deng.Exploring privacy paradox in contact tracing apps adoption[J].Internet Research,2022,Vol.32(5): 1725-1750