RedFame

Studies in Media and Communication
Vol. 10, No. 2; December 2022
ISSN: 2325-8071 E-ISSN: 2325-808X
Published by Redfame Publishing
URL: http://smc.redfame.com

Influencing Factors and Measures of Users' Privacy Disclosure in Social E-commerce

Yixuan Wu[1], Yumin Zou[1]

[1]School of English for International Business, Guangdong University of Foreign Studies, Guangzhou, China

Correspondence: Yumin Zou, School of English for International Business, Guangdong University of Foreign Studies, No.2 Baiyundadaobei, Guangzhou, China.

Received: May 25, 2022 Accepted: June 17, 2022 Online Published: June 21, 2022

doi:10.11114/smc.v10i2.5617 URL: https://doi.org/10.11114/smc.v10i2.5617

Abstract

This paper integrates Utility Theory and Communication Privacy Management Theory to explore the influencing factors of privacy disclosure in social e-commerce scenarios. The aim of this research is to provide references to optimize service for platform operators and encourage users to participate in content creation. Social e-commerce websites are the platforms based on social networking. It shortens the distance with consumers and promote e-commerce transaction activities. However, the leakage of personal privacy on the platform has cracked down on the willingness of users to disclose information. This paper collects sample data through questionnaire survey for analysis. Based on users' psychology, suggestions are given on upgrading data encryption technology to strengthen platform image marketing and give information management rights to users. It is found that perceived revenue, perceived information control and trust stimulate users' privacy disclosure, while perceived risk suppresses user's privacy disclosure in social e-commerce website.

Keywords: social e-commerce, privacy disclosure willingness, utility theory, communication privacy management theory

1. Introduction

Social e-commerce generally refers to the behavior of users joining in social interaction and sharing information that affects the sale of goods on the basis of social media. The emergence of social media not only shortens the distance with consumers, but also applies social elements such as attention, sharing and interaction to the process of e-commerce transactions to help customers make purchase decisions (Wu, 2015). With the rapid progress of technology and society, people stress the spiritual needs and material needs in an equally important position. As a platform to provide interaction and online transactions, social e-commerce website meets both needs to a certain extent.

Social e-commerce integrates the attributes of social networking and commerce. As the role of users, it gradually changes from the original passive information recipient to active information transmitter and publisher. They establish social relationships with other users through comments, feedback, interaction, and other ways while affecting their purchasing decision behaviors of products. But the process contains the risk of personal information leakage. In the e-commerce environment, platform operators can collect and analyze the data and information to grasp the behavior rules of users online (Liu, 2016). Zhou & Wang (2017) takes Alibaba and Amazon as an example that two websites collect information shared proactively by users. So users also have concerns of privacy disclosure on social media. Social media is gradually showing a trend of publicity. The content that users share on it faces the risk of being viewed and disseminated by strangers. It even becomes the goods for buying and selling (Li & Hang, 2019). Take SONY's breach of privacy information as an example, which leaked the personal information of 50 million users. Over 100 million users were affected and trapped in a "data quagmire". These actions greatly damage users' personal privacy (Dai, 2015).

The serious consequences of privacy disclosure have pushed users to focus on privacy. They treat the disclosure of personal privacy on social media cautiously. This partly hinders content production on social media and weakens the vitality of platform. This will reduce the commercial value of the platform, which is not conducive to update iteration for social media (Li, et al., 2021). From the perspective of users, reducing privacy disclosure is also not beneficial to the development of social relationships and personalized experience. Therefore, it is important to study the influencing factors of users' privacy disclosure in social e-commerce for both platforms and users. On one hand, it helps the platform better understand the psychology of users' privacy disclosure. Following it, the platform can continuously amend the privacy policy and optimize the privacy protection mechanism, which will create a more secure and harmonious social e-commerce platform. On the other hand, it provides a good chance for users to transmit information and expand social relations on social media.

At present, many scholars have explored the factors affecting users' privacy disclosure in social media or other e-commerce environments. In social media, Li & Wang (2015) combines planning behavior theory and structural equation modeling. Their research shows that perceived risk, perceived benefits and trust strongly influence users' willingness to disclose personal information. Besides, Shen (2017) uses Protective Motivation Theory to conclude that privacy risk assessment of social network affects privacy concerns and corresponding protective behaviors. In terms of e-commerce, Cao et al. (2015) conducts validity and reliability analysis. According to equation modeling, it was found that trust has a great impact on college students' willingness to shop online. Yang (2014) also found that the attributes of social networks generally influence the trust of e-commerce consumers. However, there is a lack of research on users' willingness of privacy disclosure in the background of social e-commerce. It makes a negative difference to the protection of users' personal rights and interests, which reduces their willingness and depth of participating in interactions. It also has a lagging impact on the development of operators. This will impede the progress of service upgrading and content innovation for social e-commerce platforms.

This paper will apply four factors, namely, perceived risk, perceived benefit, perceived control, and perceived trust in the social e-commerce background based on previous literature research. Data is collected by issuing questionnaires to further analyze the impact of these factors and then deeply understand users' willingness and behavior of privacy disclosure in social e-commerce platforms. So it provides the direction for the platform to take effective measures of privacy protection. It helps the platform implement standardized operation and improve the service level as well. At the same time, users' willingness is enhanced to use social e-commerce platforms to enrich the creation of interactive content and offer diversified opinions for transaction decisions.

2. Literature Review

2.1 Privacy Paradox in the Information Era

The current behavior of countless netizens keen to share personal information on the platform has gradually changed the original nature of privacy and give birth to a paradoxical phenomenon, privacy paradox. Warren & Brandeis (1890) defines privacy as the right to be alone "without interference" or "free from intrusion". On the issue of privacy, there are two different views. One believes that privacy is a basic right owned by people, which passively defends against others interference with one's private life; the other believes that privacy is another right that is derived from basic rights and has instrumental value (Xue & Chen, 2015). However, in the era of big data, virtual networks have changed the attributes of privacy. Shared privacy can meet the needs of individuals in terms of entertainment and interpersonal communication. On social media, users regard personal privacy as a commodity in exchange for perceived benefits (Li & Yu, 2018). Such privacy disclosure behavior refers to any information related to themselves conveyed by individuals (Zhong & Xu, 2019). With the change of traditional concepts, the neglect of privacy rights and the realization of network flow, users choose to disclose privacy in cyberspace, showing the paradox of privacy that someone who cares about privacy rights is willing to share privacy (Lu, 2022).

The "privacy paradox" of social networks reflects the current situation that users worry about the negative impact of privacy leakage but lack practical actions (Reibling, 2003). Influenced by users' personal characteristics, social environment, social network experience and other factors (Shen, 2017), seemingly contradictory and complex behaviors hide users' consideration of privacy disclosure: the benefits and risks of privacy disclosure, trust in platforms and other users, and the ability to control privacy boundaries. At the same time, they change users' willingness to disclose privacy and protection actions after privacy disclosure.

2.2 Influencing Factors of Privacy Disclosure Intention

User's privacy disclosure is a balanced and dialectical process between information disclosure and hiding (Wu, 2015). In social e-commerce, users' willingness to disclose privacy can be explained according to Utility Theory and Communication Privacy Management Theory. Utility Theory refers to how users look at utility and cost before making a decision that users decide whether to disclose personal information after measuring the relationship between risk and benefit (Sun et al., 2017). Communication Privacy Management Theory is a systematic theory that studies the decision-making of users to disclose or hide personal information. As two cores of Communication Privacy Management Theory, control and trust are the key factors affecting the change of privacy boundary that cannot be ignored (Guo et al., 2019)

2.2.1 Benefit-Risk

Firstly, users' decisions on whether to disclose information are affected by perceived risk and perceived benefit on social media. Perceived risk, as an inhibitory factor, affects users' willingness to disclose information negatively (Cheng et al., 2020; Han et al, 2022), while perceived benefits positively affect privacy disclosure behavior (Li & Wang, 2015; Sun et al., 2017; Guo et al., 2019). Therefore, when balancing risks and benefits and believing that the perceived benefits obtained exceed the perceived risks, users will disclose their personal information (Wu, 2015; Zhang et al., 2018; Zhuo et al., 2021).

On social media, most of the perceived benefits of users come from the sense of integration and pleasure brought by sharing information with others (Guo et al., 2019). In most cases, what users directly see is to establish a relationship with others when disclosing information. Users believe that self exposure will promote understanding and capture other parties' affection (Wang & Li, 2016). Such self exposure can be view as a kind of social exchange. Social exchange is an action laying the foundation for expecting and obtaining returns (Zheng, 2004). For users on social media, the disclosure of personal information is an important condition for gaining friends and attention (Nie & Luo, 2013). As a result, users disclose their personal privacy with the expectation of establishing new relationships, which can advance comfortable communication and acquire warmth.

2.2.2 Control-Trust

Users' disclosure of privacy also relies on the ability to control privacy boundaries and trust in the platform and other users. Depending on the Information Boundary Theory proposed by Petronio (2002), everyone will build a virtual information space, that is, information boundary. When external forces affect the boundary, individuals will trigger the sense that the privacy space is violated and attempt to control the privacy boundary (Zhang & Gan, 2021). They pay more attention to the collection and usage of privacy information (Stewart & Segars, 2002). On social media, perceived control means that users have the ability to control the privacy boundary. When individuals have the ability to control the published information according to their own wishes, they have greater autonomy to control the privacy boundary. It will unconsciously reduce their awareness of self-protection, so as to enhance their willingness to disclose privacy (Li et al., 2021). According to the theory of planned behavior, combined with Privacy Computing Theory and trust, Li & Wang (2015) proposes that perceived information control has a positive correlation with SNS users' willingness to disclose personal information. As a result, when users have higher perceived information control, they will be more confident in their ability to protect information privacy and more willing to disclose privacy.

The dimensions of collection and cognition affect and reflect users' sense of trust to a certain extent (Malhotra et al., 2004). Niu & Meng (2019) divides trust into social media trust and network interpersonal trust, that is, trust in service providers and trust in other user members (Li et al., 2021). Under the influence of trust mentality, users will reduce the uncertainty of privacy risk perception and the cost of using social media (Cheng et al., 2020), and boost the willingness of privacy disclosure. When users perceive their audiences in the information disclosure circle reliable and trustworthy, they will disclose more in-depth private content to expand their influence in the social circle and meet social needs (Zhang & Li, 2019). Trust and control jointly determine the decision-making behavior of user privacy disclosure from mentality and behavior.

2.3 Research Questions

At present, research concerns more about social media than the emerging scene of social e-commerce. However, with the continuous prominence of convenience and entertainment of virtual network, such platforms are constantly updated, iterated and widely used. Users' privacy disclosure including content release, interactive communication and online transaction is more frequent. As a result, it is urgent to carry out research on user privacy disclosure in the scenario of social e-commerce platform. From this perspective, this research will verify the impact of risk-benefit and control-trust on users' willingness to disclose privacy in the social e-commerce environment, and intend to address the following two questions:

1) Whether risk, benefit, control and trust factors affect users' willingness to disclose privacy?

2) How do risk, benefit, control and trust affect users' willingness to disclose privacy?

To settle these questions, this paper collects users' data through questionnaires in a comprehensive and systematic way, so as to lighten platform management countermeasures by analyzing the influencing factors of users' privacy disclosure. Moreover, these deep analyses can inspire effectively design the user-centered and innovative social e-commerce environment. Such a dynamic environment greatly provides users with better socialization and shopping-service experience and builds a green and active platform ecology, which will afford the possibility for the platform to maintain users and expand its scale.

3. Methods

The questionnaire of this study revolves around the influencing factors of users' willingness to disclose privacy in social e-commerce, including four independent variables: perceived risk, perceived benefit, perceived control, perceived trust in addition to one dependent variable: willingness of privacy disclosure. In terms of the design of the questionnaire, the questions in this study are used or adapted from previous studies (e.g., Guo et al., 2019; Jiao, 2019; Yu, 2020). At the same time, it is combined with the actual situation of the social e-commerce platform to make changes. The options in the questionnaire are available on the Likert Level 5 scale (1= very disagree, 2= disagree, 3= general, 4= agree, 5= very agree).

In order to promote the respondents' understanding for the content of the questionnaire, the questionnaire begins with a brief introduction of the survey and explains some keywords, such as *what is a social e-commerce platform*. 20 users who have used social e-commerce platforms are invited to fill in the questionnaire as a forecast test before the research. According to their feedback, the question statement will be modified. The questionnaire items are as follows:

Table 1. Questionnaire Design

Variables	Questions
Perceived Risk	1. be abused private information
	2. lose important property
	3. leak related privacy
	4. be reluctant to continue providing personal information when realizing the risk of disclosure
Perceived Benefit	1. enjoy the desired service
	2. build friendly relationship
	3. be willing to provide more personal information when gaining returns
	4. be willing to provide more personal information when realizing benefits exceed risks
Perceived Control	1. master the use of information
	2. know the scope of collected information
	3. be willing to provide more personal information when possessing information control
Perceived Trust	1. believe in interacted users
	2. comply with the privacy protection items
	3. be safeguarded against dangers
	4. be willing to provide more personal information when trusting operators and other users

The questionnaire is designed through the network platform and distributed on wechat, QQ and other online platforms. After eliminating the samples with consistent answers and short filling time, a total of 183 valid questionnaires have been collected. These questionnaire data will be thoroughly analyzed below.

4. Data Analysis and Discussion

4.1 Validity and Reliability Analysis

Validity and reliability analysis are mainly used to measure whether the design of research items is effective to know the direct relationship between variables and whether the research data is reliable. Only when the validity and reliability meet the standards, can the questionnaire be proved to be reliable, and the subsequent data analysis can be carried out.

4.1.1 Validity Analysis

Validity reflects the accuracy of item design and the validity of measurement results (Guo et al., 2019). In this study, KMO and Bartlett tests are used to verify the validity. KOM value and the Communality index are adopted to verify the validity level of the data. The KOM value judges the degree of suitability for factor analysis. The value is usually higher than 0.6. If it is greater than 0.8, it means that the research data is very suitable for extracting information. The degree of Communality reflects the amount of information that can be extracted. Normally, Communality's standard is 0.4. The statistical results show that the validity of the questionnaire in this study is outstanding. It's very suitable for extracting information (Table 2), because the Communality value to all the research items is higher than 0.4, indicating that the information can be effectively extracted. And the KOM value is 0.934, which also means that the validity is good. And the P-value is 0.000 (Table 3), less than 0.05. Furthermore, it has passed the Barth's sphericity test, which also gives evidence to support valid questionnaire.

Table 2. Validity and Reliability Index

Variable	Communality	Corrected Item-Total Correlation (CITC)	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
PR1	0.858	0.807	0.949	0.953
PR2	0.876	0.793	0.949	
PR3	0.906	0.824	0.948	
PR4	0.769	0.741	0.951	
PB1	0.622	0.659	0.952	
PB2	0.625	0.675	0.952	
PB3	0.664	0.834	0.948	
PB4	0.598	0.712	0.951	
PC1	0.718	0.736	0.950	
PC2	0.719	0.744	0.950	
PC3	0.650	0.657	0.952	
PT1	0.813	0.755	0.950	
PT2	0.782	0.716	0.951	
PT3	0.789	0.758	0.950	
PT4	0.703	0.785	0.949	

Table 3. KOM and Bartlett Test

KMO test	KOM	0.934
Bartlett's Test of Sphericity	P-value	0.000

4.1.2 Reliability Analysis

Reliability reflects the consistency of the results obtained (Guo et al., 2019). In this study, the commonly used Cronbach α coefficient is used to measure the reliability of the sample responses. Generally, it is considered that the reliability is acceptable if it is greater than 0.6, and the reliability is acceptable if it is greater than 0.8. It can be explained that the reliability is high. At the same time, CITC is combined to test the degree of correlation between the analysis items and the deleted alpha coefficient to test whether the analysis items are necessary to make the reliability analysis more comprehensive. It can be seen from Table 2 that α coefficient is 0.953, which is higher than 0.9, indicating that the reliability of the research data is high. In addition, the CITC value generally only needs to be higher than 0.4. The CITC values of the data collected by this questionnaire are all greater than 0.6, suggesting that there is a correlation between the analysis items, and α coefficients of the deleted items are also lower than the α coefficient, proving that all the items are necessary to exist. Therefore, the data collected by this questionnaire has good reliability.

4.2 Questions Test

To answer the questions raised in this study, the researchers use Pearson's correlation coefficient to analyze the correlation between variables of the collected data, which are the effects of perceived risk, perceived return, perceived control and perceived trust on disclosure intention.

4.2.1 Perceived Risk

From Table 4, it can be seen that the P-value of perceived risk and unwillingness to disclose privacy are all equal to 0, less than 0.05, presenting that there is a significant linear correlation between perceived risk and willingness to disclose privacy. Furthermore, the correlation coefficients are both greater than 0.7, pointing out not only strong correlation, but also a positive correlation. When users perceive risks, they are reluctant to disclose privacy, so there is a statistically significant negative relationship between perceived risks and willingness to disclose privacy.

According to Protection Motivation Theory, when facing risks, people will have four cognitive evaluation processes:

evaluating the severity of hazards, evaluating the possibility of hazards, evaluating the ability to deal with risks, evaluating the ability to take corresponding actions. After evaluations, people take corresponding steps to protect themselves (Shen, 2017). Based on this, the main reasons why users' willingness to disclose privacy and perceived risk are negatively correlated are as follows:

First, users use a social platform with e-commerce attributes, so users' information will inevitably involve sensitive information, such as financial information including bank accounts. Once the user's privacy is leaked, it may cause irreparable losses to the user's property. Money loss is undoubtedly an extremely serious consequence for users. Therefore, under the assessment of hazard severity, users are more sensitive to perceived risks. Filled with alarm at the perceived risks, they are be discouraged to disclose privacy. Second, prevalent big data and innumerable users who are active on the platform provide a certain hotbed for privacy disclosure. Because the privacy information disclosed by users may be disseminated to thousands of people through big data, People have the opportunity to master these privacy information and abuse it to harm users who reveal their privacy, such as illegally selling information to the third party, monitoring users who disclose information, etc. According to incomplete statistics, there were millions of cases involving privacy data disclosure, and billions of people fell under the influence of it. Therefore, privacy disclosure is explosive and universal (Jin, 2020). In view of the great possibility of privacy disclosure, users will deal with the risk more carefully. Third, with the blessing of cloud computing, the flow and dissemination of information are much faster than before. Once the risk occurs, it may be beyond the control of users. Worse, privacy disclosure is often instantaneous so it is difficult to remedy the situation by the user's own power. Therefore, in the face of such a situation, users may tend to avoid disclosing privacy after measuring and finding that their ability to deal with risks and rescue is limited.

Since perceived risk has a significant impact on user's willingness to disclose, so relevant social e-commerce platforms should take measures to reduce user's perceived risk. Firstly, under the banner of adhering to the business philosophy of integrity and morality, the platforms can clarify that they will not abuse users' information or open a "data back door" to the third parties to reduce the possibility of privacy disclosure. Secondly, the platforms strengthen their own technical management to allow users to disclose information anonymously and avoid dangers such as Internet mass hunting and information matching. In addition, the platform should be vigilant about its own recommendation services, because social media recommendation does not always make users feel convenient or satisfy users' demand as we suppose. On the contrary, sometimes it will cause users' disgust. Zhang & Gan (2021) has found that social media recommendation has a positive impact on perceived privacy risk. When the services recommended by the platform are more accurate to match users' preferences, it reflects the information-mastering differences between the platform and users, which undoubtedly stimulates users' awareness that information is collected by the platform, reduces users' sense of security and raises their sense of crisis. In spite of these, recommendation service has certain advantages. Account of two sides of recommendation service, platforms had better exert adequately the leverage of it to avoid abuse and increasing the perceived risk of users.

Table 4. Unwilling to Disclose Privacy

X→Avoidance of disclosing privacy	Correlation coefficient	P-value
PR1	0.747	0.000
PR2	0.763	0.000
PR3	0.796	0.000

4.2.2 Perceived Benefit

As shown in Table 5, perceived benefit has a significant positive correlation with privacy disclosure, because the correlation coefficient is more than 0.6, and P-value is less than 0.005. When users perceive that disclosing information on the platform can bring multi-dimensional benefits, they will tend to disclose their information. Due to the dual attributes of social networking and shopping, the platforms offer a pleasant experience of shopping and sharing (Wu, 2015). The perceived benefits of such harmonious interaction, convenient shopping, and building a relationship network spur users to disclose information.

This positive relationship also enlightens management for the platforms. If platforms want to further dig out the vitality, improving the perceived benefits of users can be as a breakthrough. The platforms can push the moments shared by users to more users, which promotes interaction between users. Platforms can also encourage users to disclose more information about purchased products to attract other users, boosting other users shopping pleasure by finding suitable products faster.

The social e-commerce platform is different from daily offline contact, it is aimed at a wider and more unknown group of people. For this reason, users are exposed to more strangers with different traits and personalities so the information disclosed on the platform is more likely to be embraced. Users can release their pressure and achieve self-expression by sharing "good things" or other experiences. Apart from spiritual benefit, self-disclosed users may also gain material benefits if developing well, because merchants will pay these users with a large number of fans to advertise their products. This is an interactive and mutually supportive relationship that benefits not only the discloser, but also the receiver. Reciprocity is one of the conditions for continuous and in-depth social communication and maintain relationship (Liu, 2019). Sharing as medium creates a bridge for disclosers and receivers to establish social relations, but also gain what they need. The discloser fulfills the spiritual needs of revealing ideas, and the information receiver fulfills the need to obtain ideal product information. Therefore, the platforms need add exposure to users' disclose information to realize mutual benefit perception.

No matter what kind of benefits it is, the platform should grasp it well to form a good cycle in which disclosure willingness brings better experience, and better experience promotes disclosure willingness. In this regard, the approach of the RED platform is a good example. As a "grass-growing artifact" for young consumers, RED first appeared as a shopping and sharing community, and later upgraded to e-commerce, adhering to the fine genes of "sharing beauty" all the way to achieve a perfect closed-loop transaction of the grass-growing model. The essence of "growing grass" is social marketing, which uses social relationships for commercial consumption (Jiang & Chen, 2019). RED makes full use of the inherent attributes of "growing grass" to improve users' stickiness and benefit perception. Anyone can write the content on RED. As long as the content is of high quality or owns a lot of likes and favorites, it may become popular. Against the background of this mechanism, users are keen to share and "grow grass" on it. Naturally, it benefits other users to search for a lot of related product notes. Individuals interact with others in the RED community, such as likes and comments, to obtain resources provided by others, and thus feel the resources brought by the platform. Meanwhile, in the principle of strengthening their social capital in the communication community, individuals are also willing to continue to "grow grass", and form a virtuous circle (Liu, 2019). Therefore, RED applies the mechanism of users disclosing privacy to maintain the vitality of the platform.

4.2.3 Perceived Control

Perceived control has a positive correlation with disclosure willingness as well, but the degree is not as strong as perceived benefit, because the correlation coefficient between perceived control and disclosure willingness is between 0.4 and 0.6 (Table 5), which is a moderate correlation. Perceived benefit is a relatively intuitive and easy-to-obtain feeling, the users can clearly feel the fun of the interaction between users and the convenience of shopping choices, while the perceived control is a relatively vague feeling. Users at the center of the platform's usage diminishes the possibility to clearly monitor whether the disclosed information is within users' own control. For instance, when one user's information disclosed in the platform is plagiarized by others and disguised as their image to attract fans, this user does not realize it. This example reflects that users probably do not identify that the information is out of control.

Although the perception of information control is a bit hazy for users, it is undeniable that this still has an effect on users' willingness to disclose. Between the public and individual, there is a privacy boundary built on the basis of social norms (Li & Yu, 2018). In this privacy boundary, users expect that they have the right to control their private information. Under the theory of planned behavior, the user's ability to control personal information directly affects the disclosure decision (Sun et al., 2017). When users own cognition that they have certain control over information, they may feel more at ease and are more willing to expand the boundaries of information privacy. That means they reduce the perceived risk (Guo et al., 2019), thereby enhancing the willingness to disclose privacy. According to this, the platforms release more information control rights to users. For example, users can choose whether to disclose information to enterprises, or who can access the information disclosed by users, so as to reduce users' concerns about information security and the negative impact of information collection on users (Jiang et al., 2021). Alibaba in China and Amazon in the United States use privacy policy descriptions to improve users' perception of information control. Both promise users that information will only be shared with third parties after obtaining users' consent or out of service needs, etc. They will inform users about the purpose of collecting information (Zhou & Wang, 2017), which reveals a sign that users participate in controlling information and have a certain right to speak. So it declines their concerns about the collection of information by the website. Alternatively, the platform can have anonymous publishing settings for needed users to choose. Users can control their identification (Li et al., 2021) through anonymity. If users are sensitive to information control and direction of outflow, anonymization gives such users the option to control information to a certain extent, which is a practical method.

4.2.4 Perceived Trust

There is a strong positive relationship between trust and privacy disclosure, and the correlation coefficients are all greater than 0.6 (Table 5). As a positive psychological state, trust will play a certain positive role in user decision-making. When users perceive that the platform and other users are trustworthy, they will reduce their alertness, feel comfortable within the boundaries of disclosure privacy. They will not worry about disclosing information, which means that reduce risk perception (Guo et al., 2019). As previously studied, perceived risk inhibits the willingness to disclose privacy, and users' trust can relieve perceived risk, so it is not unexpected that trust positively affects privacy disclosure. When users have established trust in websites and other users, they may not only disclose information, but also tend to disclose real and non-forged information (Nie & Luo, 2013). It is undoubtedly beneficial to the platform. When more and more users are delighted to disclose real information, other users who interact with it will be motivated unconsciously after they recognize this. On the contrary, if the user discloses processed or false information, other users will unconsciously feel that the person untrustworthy. So the platform and other users on the platform are viewed with suspicion, which is not conducive to mutual trust building, and even bring about a vicious circle, resulting in the collapse of trust.

Since building trust has such a strong effect on willingness to disclose, platforms has got to consider to effectively increase users' trust. Two objects of trust should be used as benchmarks: the platform and the active users on the platform. The first one is that the platforms create a safe and private environment, which is conducive to users' disclosure behaviors to a higher degree (Zhang & Li, 2019). When users disclose information on the platform, it entails opening their hearts. If the environment does not impose any restrictions, users will adopt defensive mechanisms instead of being honest. In order to put down users' precautions, it is necessary for the platform to increase technological research and development, such as upgrading data encryption technology and enhancing data privacy protection (Wang, 2019). Second, the platforms emphasize its own brand image. In the early stage, the platform can spare no effort on image marketing to improve the familiarity and goodwill of potential or existing users to the platform. Nie &Luo's (2013) research points out that familiarity can stimulate users' trust in the website, and favor as a positive psychological state can mobilize users to do positively corresponding activities, such as spending more time on the platform. For active users on the platform, the platforms need to increase their control over them, including detecting offensive remarks and behaviors to avoid friction in the social area or shopping area, which poses a potential threat to other users' cognition. Only by grasping the ethos of the platform itself can users be guided to develop a stable and lasting sense of trust after familiarizing themselves with the platform. Otherwise, it is difficult to ensure long-term trust if only focusing on image marketing.

Table 5. Willing to Disclose Privacy

X→Intention of disclose privacy	Correlation coefficient	P-value
PB1	0.633	0.000
PB2	0.681	0.000
PC1	0.573	0.000
PC2	0.415	0.003
PT1	0.699	0.000
PT2	0.692	0.000
PT3	0.709	0.000

5. Concluding Remarks

From the perspective of privacy behavior itself and user's personal cognition, this study integrates Utility Theory and Communication Privacy Management Theory. It attests and learns the role of perceived risk, perceived benefit, perceived control, and perceived trust on user privacy disclosure in social e-commerce. In conclusion, the perceived risk suppresses users' disclosure willingness, while perceived benefit, perceived information control and perceived trust boosts disclosure willingness. In addition to analyzing these factors, we offer enlightening management suggestions in term of recommendation services, business ethics, communication circle and users' rights. This research expands the occurrence scenario of users' willingness of privacy disclosure and enriches the theoretical achievements in this field. For one thing, it helps social e-commerce platforms to understand users' behavior of privacy disclosure, which is universal to improve the platform architecture. For another, it echoes users' high attention to privacy disclosure under the background of big data, and optimizes their experience. However, due to time constraints, the survey sample selection is not large. Also, the impact of individual factors such as gender, age and the degree of education on user privacy disclosure is not considered in the research. Future studies are suggested to expand the scope of survey subjects and make a concrete analysis of demographic characteristics, thus improving the refinement of research.

References

Cao, S., Guo, C., Zhang, M., Zhang, S., & Ma, X. (2015). Empirical analysis of the factors affecting mobile social e-commerce user recommendation on college students' online shopping willingness. *Business Economic Research,* (36), 61-63.

Cheng, H., Wen, X., & Su, C. (2020). Influence factor model of social media users' privacy disclosure willingness and empirical research. *Book and Information Work,* (16), 92-104. https://doi.org/10.13266/j.issn.0252-3116.2020.16.010

Dai, L. (2015). Data security risks and governance in the digital economy era. *Information Security and Communication Confidentiality,* (11), 89-91.

Guo, H., Ma, H., & Xu, Z. (2019). Model construction and demonstration of information disclosure willingness of social media users-A case study of wechat users. *Book and Information Work, 63*(15), 111-120. https://doi.org/10.13266/j.issn.0252-3116.2019.15.013

Han, Z., Shi, L., & Zhao, Y. (2022). Consider the privacy exchange behavior of APP users in different usage scenarios. *System Management Journal,* (02), 353-361.

Jiang, J., & Chen, X. (2019). Network "planting grass": social marketing, consumption induction and aesthetic fatigue. *Learning and Practice,* (12), 125-131. https://doi.org/10.19624/j.cnki.cn42-1005/c.2019.12.015

Jiang, N., Gu, F., & Li, H. (2021). Study on the relationship between information collection concern and protective motivation and protective behavior-Transparency of information use and the regulation of perceptual control. *Soft Science, 35*(3), 116-122. https://doi.org/10.13956/j.ss.1001-8409.2021.03.18

Jiao, S. (2019). Study on the influence factors of social e-commerce users (Master’s dissertation, Jilin University).

Jin, Y. (2020). On the leakage and protection of personal privacy data in the era of big data. *Journal of Tongji University (Social Sciences Edition), 31*(3), 18-29.

Li, G., & Wang, D. (2015). Research on the influencing factors of users' personal information disclosure willingness on social networking websites: Take Sina Weibo as an example. *Documentation, 36*(1), 35-40.

Li, K., & Yu, Y. (2018). Research Review and Prospect of Online Privacy Disclosure in Social Media. *Summary and Review, 41*(12), 155-160.

Li, W., & Hang, M. (2019). Privacy dilemma in social media: Privacy boundaries and big data concerns. *Friends of Editing,* (01), 55-60.

Li, X., Huang, L. H., & Chen, J. (2021). Study on the influence factors of social media users based on meta-analysis. *Data Analysis and Knowledge Discovery*, 1-12.

Liu, J. (2016). Research on the Practical Development of E-commerce Platform in the Era of Big Data-Take Taobao as an example. *Reform and Strategy,* (05), 122-126. https://doi.org/10.16331/j.cnki.issn1002-736x.2016.05.024

Liu, T. (2019). Why are young women keen to share "good things" in online communities-Analysis based on the motivation theory. *Youth Phenomenon,* (07), 91-97+112. https://doi.org/10.19633/j.cnki.11-2579/d.2019.0117

Lu, J. (2022). Helpless choice: the performance, reasons and trade-offs of privacy transfer in the digital age. *News and Writing,* (01), 14-21.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355. https://doi.org/10.1287/isre.1040.0032

Nie, Y., & Luo, J. (2013). Perceive usefulness, trust and willingness of users to disclose personal information. *Knowledge of Books and Intelligence,* (05), 89-97. https://doi.org/10.13366/j.dik.2013.05.006

Niu, J., & Meng, X. (2019). The influence of social media trust on privacy risk perception and self-disclosure: the intermediary effect of online interpersonal trust. *International Press, 41*(07), 91-109. https://doi.org/10.13495/j.cnki.cjjc.2019.07.007

Paveka, S. (2018). Social Media: Principle and Application. 12.

Petronio, S. A. I. (2002). Boundaries of Privacy: Dialectics of Disclosure.

Reibling, P. C. G. Z. M. E. G. E. T. (2003). What to Convey in Antismoking Advertisements for Adolescents: The Use of Protection Motivation Theory to Identify Effective Message Themes. *Journal of Marketing*, 1-18. https://doi.org/10.1509/jmkg.67.2.1.18607

Shen, Q. (2017). Risk-cost trade-off: the "privacy paradox" in social networks-Take the wechat mobile social application (APP) of Shanghai college students as an example. *Journalism and Communication Research,* (08), 55-69.

Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research, 13*(1), 36-49. https://doi.org/10.1287/isre.13.1.36.97

Sun, X., Cheng, Y., & Zhu, Q. (2017). Study on the influencing factors of user privacy disclosure behavior intention in social search. *Intelligence Magazine*, (10), 172-179+201.

Wang, B., & Li, Q. (2016). The privacy boundary and management regulation of wechat moments in the era of big data-Based on the theoretical perspective of communication privacy management. *Intelligence Theory and Practice, 39*(11), 37-42. https://doi.org/10.16353/j.cnki.1000-7490.2016.11.008

Wang, W. (2019). Personal privacy protection in the era of big data. *Digital Communication World,* (11), 265-266.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220. https://doi.org/10.2307/1321160

Wu, Y. (2015). Study on the influence factors of user privacy disclosure willingness in Social E-commerce. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 27*(2), 54-60.

Xue, F., & Chen, H. (2015). Exploration on the ethics of big data privacy. *The Study of the Dialectics of Nature, 31*(02), 44-48. https://doi.org/10.19484/j.cnki.1000-8934.2015.02.011

Yang, Y. (2014). Analysis of the influence of social network attribute on the trust of e-commerce consumers. *Business Times,* (25), 67-69.

Yu, D. (2020). Study on Influencing Factors of Consumer Information Disclosure in E-commerce (Master's dissertation, Southeast University).

Zhang, X., & Gan, M. (2021). Research on the influence mechanism of social media recommendation on users' online interaction intention from the privacy perspective. *Modern Intelligence, 41*(5), 33-43+103.

Zhang, X., & Li, B. (2019). Trust and risk perception: Empirical research on the influencing factors of privacy and security in social networks. *Media Education,* (2), 153-166.

Zhang, Y., Sun, X., Lu J. & Zhu, Q. (2018). Empirical research on mobile social users' willingness to disclose information based on privacy computing theory-Take wechat as an example. *Books and Intelligence,* (03), 90-97.

Zheng, L. (2004). Compare the similarities and differences between social exchange theory and rational choice theory-Take Bru, Coleman as example. A*cademic Exchange,* (01), 108-113.

Zhong, Z., & Xu, Z. (2019). Effect of information privacy disclosure in online evaluation on consumer reliability perception in online evaluation. *Information Science, 37*(9), 159-163. https://doi.org/10.13833/j.issn.1007-7634.2019.09.027

Zhou, S., & Wang, W. (2017). A Comparative study on the Privacy Policy of Sino-US E-commerce websites-Take alibaba and Amazon as example. *Modern Intelligence, 37*(01), 137-141

Zhuo, R., Jiang, L., & Fang, Y. (2021). Effect of privacy protection and self-efficacy on APP users' information disclosure willingness. *Enterprise Economy,* (04), 113-121. https://doi.org/10.13529/j.cnki.enterprise.economy.2021.04.013

Copyrights