Research on the Influencing Factors and Behavioral Mechanisms of Users' Willingness to Disclose Privacy in E-commerce Situations-Based on Grounded Theory

Hongfu Yu[1,*], Pingfeng Liu[2]

[1]School of Entrepreneurship, Wuhan University of Technology, Wuhan, Hubei, China
[2]School of Economics, Wuhan University of Technology, Wuhan, Hubei, China

*Alone7758@qq.com , 1652605258@qq.com

Abstract. With the development of e-commerce and artificial intelligence technology, privacy leakage incidents have caused concern among network users, but on the one hand, network users say that they care about their privacy, and on the other hand, they disclose their privacy. In this paper, 12 Internet users were interviewed in depth using the grounded theory method of qualitative research. The influencing factors and behavioral mechanism model of users' privacy disclosure intention are constructed by corresponding coding, and the conclusion is drawn that privacy fatigue will affect people's privacy disclosure behavior directly and indirectly by influencing perceived trust. Perceived trust has a direct impact on privacy disclosure behavior, while perceived trust and privacy fatigue are influenced by external factors, personal factors and privacy calculation,   which provides a lesson for e-commerce companies to better use AI to carry out marketing campaigns, and collect and protect customer privacy.

Keywords: E-commerce Situations; privacy disclosure; influencing factors; behavioral mechanisms.

1   Introduction

With the development of the Internet industry, the information released by users on the Internet and the traces of browsing have generated a large amount of data. Although the collection of user information can bring users personalized recommendation and convenience, it is precisely because of the personalized recommendation of artificial intelligence that users are worried about information leakage. But while people express their concerns about privacy on the one hand, they continue to disclose their privacy on the other. In view of the contradictory behavior in people's privacy disclosure behavior, it is called the privacy paradox in academia. The privacy paradox exists widely in the context of online business transactions (such as e-commerce websites) and social interactions (such as social networking sites).

   The more mainstream privacy computing theory goes through the stage of completely rational hypothesis [1] and believes that even if there is privacy risk, users are

willing to provide personal information as long as the expected benefit is greater than the cost, but it is difficult to explain the situation where the cost is greater than or equal to the benefit and the situation where the two cannot be compared. Aquis believes that people's decision to disclose privacy is bounded rationality, pointing out that the incompleteness and asymmetry of external information environment, heuristic cognition and cognitive bias are internal and external factors that affect personal information privacy decisions[2].Byoungsoo Kim and Daekil Kim (2020) incorporated the perceived control and subjective norms of personal information into the privacy computing model, proposed an innovative theoretical framework, and empironally concluded that personal privacy concerns have a negative impact on information disclosure, but it is not significant[3]. Users' trust in the platform and perceived degree of control over information have a significant positive impact on information disclosure, and a high degree of perceived control over information will ease privacy concerns[4]. Perceived trust and perceived risk will also affect users' privacy disclosure behavior People's perceived privacy risk is high, and their risk tolerance is low, so their perceived trust is low[5]. The uncertainty caused by perceived privacy risks will reduce individuals' willingness to disclose private information[6].

In recent years, some scholars have used the newly developed privacy fatigue theory to explain the privacy paradox. Based on the feature fatigue theory, Keith et al. verified the existence of Internet users' privacy fatigue by experimental methods[7] Choi et al.(2018) further defined the connotation of privacy fatigue, believing that privacy fatigue is a multi-dimensional concept, including emotional exhaustion and cynicism[8]. User privacy fatigue is positively correlated with privacy disclosure intention and privacy withdrawal behavior However, excessive fatigue may induce disengagement behavior [9].

On the basis of the above researches, this study focuses on the psychological development of users and the influence process of external environment, adopts the qualitative research method of grounded theory to conduct in-depth analysis and research on the influencing factors and behavioral mechanisms of Internet users' privacy disclosure intention, and explores the key influencing factors and their interactions. The hope is to provide new ideas for e-commerce companies to take into account user privacy ethics and development when using artificial intelligence technology.

2   Research Methodology and Data Preparation

2.1   Research Methods

the paradox of online users' privacy disclosure in the context of e-commerce has attracted academic attention, but academics have not yet formed a unified research framework for the study of privacy paradox. Qualitative research is a bottom-up approach to constructing theories based on social phenomena, which is suitable for exploring and analyzing newer fields. Therefore, this study will adopt the qualitative research method, based on the rooted theory, to collect data through in-depth interview method, to explore the factors affecting online users' hidden disclosure, to analyze the path of action

between each factor, and to explain the behavioral results of users' privacy disclosure[10].

2.2   Sample Selection

Teenagers, college students and postgraduates are the main users of the Internet, so this study selects 12 postgraduates as the interview objects. Interview principles should be strictly observed during the interview. 3. Category Refinement and Modeling

3   Category Refinement and Modeling

3.1   Open coding

In this study, 26 representative raw data statements were formed during the open coding process. After further summarization, 18 concepts were obtained and integrated into 13 initial categories. The results of the specific open coding study are shown in Table 1.

Table 1. Results of open coding

Open Coding Categoryization		
Beginner's category	Conceptualization	Primitive statements
B1 user experience	A1 privacy leakage experience	a1 have encountered privacy invasion incidents related to the Internet, browsing records on one software will be known by another software, especially online shopping platforms as if they know your search records, accurate recommendation
		a2 always receive some harassing phone calls, that is, after I have disclosed a certain merchant or app in the online shopping, then I will receive
		a3 After buying something on Taobao, the merchant always sends me a text message and calls me
……		

3.2   Spindle Coding

Based on the 13 initial categories formed by open coding, six main categories are formed after analyzing their internal logical relations, as shown in Table 2.

Table 2. Spindle codes

Spindle code results	
Master Scope	Initial Scope
C1 Privacy fatigue	B9 Emotional exhaustion
	B10 Cynicism
C2 Perceived trust	B3 Risk control
C3 Willingness to disclose privacy	B11 Protective behavior
	B12 Withdrawal behavior
C4 Individual Factors	B1 User Experience
	B2 privacy literacy
	B13 Self-protection efficacy
C5 Privacy calculations	B6 Perceived benefits
	B7 Perceived Costs
C6 External factors	B5 Supervision and management
	B8 Service overload
	B4 Group factors

3.3   Selective Coding

The results of selective coding in this study are shown in Table 3. After conceptual coding and in-depth analysis in the early stage, we drew a theoretical framework diagram of the influencing factors and influencing paths of Internet user privacy disclosure, as shown in Figure 1.

Table 3. Selective coding

| Typical structure	Relational structure	Connotation of relational structure
External Factors→Privacy Fatigue	Causation	External factors are external factors that trigger privacy fatigue
Personal factors→Privacy Fatigue	Privacy Fatigue	Personal factors are internal factors that trigger privacy fatigue
Privacy fatigue→Perceived trust	Intermediary	Increased privacy fatigue increases users' mistrust of e-commerce platforms, leading to a decrease in users' willingness to disclose their privacy
Personal factors →Perceived trust	Intermediary	Personal factors are internal factors that influence users' trust in e-commerce platforms
Privacy calculations→Perceived trust	Causation	Users decide whether to trust the platform by calculating benefits and costs
Privacy calculations→Perceived trust	Causation	External environment affects users' trust in e-commerce platforms
Privacy fatigue→Privacy disclosure willingness	Causation	Privacy fatigue causes users to adopt exit behavior and forces them to adopt privacy disclosure
Perceived trust→Privacy disclosure willingness	Causation	Users who distrust the e-commerce platform will adopt protective behaviors and reduce information disclosure
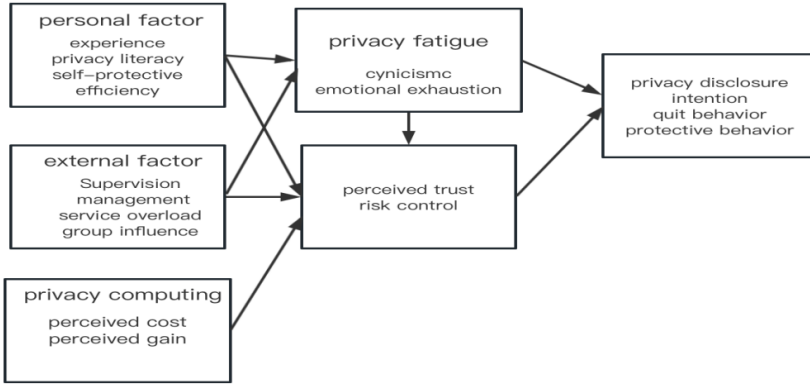
Fig. 1. Model of user privacy disclosure mechanism

3.4   Theory Saturation Test

In the remaining 2 samples analyzed, no new categories were created and no new relationships between categories were created. As a result, it can be concluded that this rooted theory study met the requirements of the theory saturation test.

4   Conclusion

In this study, through three steps of open coding, spindle coding and selective coding of rooted theory, the factors in the path of users' privacy disclosure are summarized into six variables, and different variables have different paths of influence on users' willingness to disclose privacy[11]. The following is a description of the path of each variable on the willingness to disclose privacy.

4.1   Influence of Personal Factors on Privacy Fatigue

Personal factors have an important impact on privacy fatigue, including user experience, self-efficacy and privacy literacy. Users who have experienced privacy leakage events have a high degree of privacy fatigue tolerance, and if too many privacy leakage events make people feel strong privacy fatigue and have no energy to take care of others, users' privacy fatigue will reach the peak. Users' privacy literacy also has an impact on privacy fatigue[12]. When users have a low level of privacy protection skills and are highly concerned about their privacy, they are more likely to experience privacy fatigue if they encounter too many privacy disclosure incidents, while users with low privacy concern are not easy to have privacy fatigue. Users with a high sense of privacy internal self-protection efficacy are not prone to privacy fatigue, and they believe that they can protect their privacy well, while users with a high sense of external self-protection ef-

ficacy usually have a certain degree of privacy fatigue, believing that the external environment will not effectively protect their privacy, resulting in cynicism in privacy fatigue

4.2   External Factors will also have an Impact on User Privacy Fatigue

External factors include supervision and management, service overload and group factors. It is found in the interview that when users encounter privacy invasion and unreasonable privacy terms, they have no success in seeking help, and the perception that personal strength cannot fight against large e-commerce companies will produce obvious privacy fatigue, and the accumulation of privacy fatigue will produce a strong sense of emotional exhaustion for users[13]. External groups will have an important impact on the formation of individual beliefs. Some users said in the interview that they used to worry about their privacy protection, but their friends said nothing, so they also formed such a concept, no longer tired of protecting their privacy, and the sense of privacy fatigue has weakened a lot.

4.3   Personal Factors will affect Perceived Trust

Perceived trust is manifested through the risk control of network users, and the better the perceived risk control of users, the higher the perceived trust will be. Risk control includes risk tolerance and risk prediction. The interview found that when users experience more privacy disclosure events, risk tolerance will decrease, risk prediction will be more vigilant, and perceived trust will decrease[14]. In privacy literacy, poor privacy protection skills and poor self-protection effectiveness tend to lead to low perceived trust, low privacy concern, and less attention to their own privacy protection, they are less likely to pay attention to risks, and high perceived trust.

4.4   Influence of External Factors on Perceived Trust

Good external supervision conditions will reduce the perceived risks of network users, make them think that the illegal cost of Internet manufacturers is higher, and the possibility of violating users' privacy is less, and the perceived trust will increase[15]. However, the mandatory personal information acquisition terms of apps or platforms will cause users to make bad assumptions, resulting in increased risk prediction and decreased trust. In addition, the perceived trust degree of the surrounding friends will also affect the perceived trust degree of the user.

4.5   Impact of Privacy Computing on Perceived Trust

Users' perceived trust in a platform and app is affected by the calculation of users' perceived benefits and perceived costs of the platform. It is found in the interview that the platform or app can reduce the perceived risks of users and increase the perceived trust by meeting the needs of customers and increasing the perceived benefits of customers.

4.6   Influence of Privacy Fatigue on Privacy Disclosure Intention

Privacy fatigue includes emotional exhaustion and cynicism. Emotional exhaustion means that users are exhausted from protecting their privacy. Cynics argue that efforts to protect privacy are ineffective. Through interviews, almost all users with privacy fatigue said that privacy fatigue will cause their acquiescence to apps or other manufacturers to obtain their privacy rights to a certain extent, resulting in patient behavior and increased willingness to disclose privacy, and even serious privacy fatigue, especially cynicism will cause users to ignore privacy Settings and other issues and conduct privacy disclosure behavior[16]. However, in the interview, most users with privacy fatigue also said that even if they feel privacy fatigue, they will not completely give up the protection of privacy, even if they acquiesce in privacy disclosure, they will still protect the deep-seated privacy content, and they also said that the perceived trust decline caused by privacy fatigue, or even aversion, leads to the privacy protection behavior. Therefore, privacy fatigue will not only cause patience and neglect of privacy disclosure intention, but also affect users' protective behavior through another path, which affects perceived trust.

4.7   Influence of Perceived Trust on Privacy Disclosure Intention

Perceived trust will affect users' privacy disclosure behavior, including users' trust in others and social platforms. The higher the degree of trust users have in people and social platforms, the less concerns they have about the abuse of personal privacy, and the more inclined they are to have withdrawal behavior - to entrust privacy protection to the e-commerce platform, so as to voluntarily disclose their privacy.

In summary, under the trend of increasingly strict information security protection law, it is difficult for users to reach the second stage of privacy fatigue. Therefore, the violation of user privacy by e-commerce platforms will lead to a decline in user trust, prompt users to have protective behaviors, and reduce their willingness to disclose privacy, thus leading to a decline in the preference data obtained by e-commerce platforms from users. The platform's behavior of respecting user privacy will increase users' perceived trust and willingness to disclose.

References

1. Lee N., Kwon O. A 2015.Privacy-Aware Feature Selection Method for Solving the Personalization-Privacy Paradox in Mo- bile Wellness Healthcare Services[J].Expert Systems with Ap- plications, 42(5):2764-2771.
2. Alessandro Acquisti, Laura Brandimarte & George Loewenstein, 2015.Privacy and human behavior in the age of information, 347 Science 509, 514 (2015).
3. Byoungsoo Kim, Daekil Kim. 2020.Understanding the Key Antecedents of Users' Disclosing Behaviors on Social Networking Sites: The Privacy Paradox[J]. Sustainability,12(12):
4. Piper B. F., Lindsey A. M., Dodd M. J.1987.Fatigue Mech- anisms in Cancer Patients:Developing Nursing Theory[J].Nursing Forum, 4(6):17-23.

5. Shirom A. Burnout in Work Organizations [M].New York:Ohio Geological Society, 1989:25-48.

6. Marcora S. M., Staiano W., Manning V. Mental Fatigue Impairs Physical Performance in Humans[J].Journal of Applied Physiology, 2009, 106(3):857-864.

7. KEITH M J, MAYNES C, LOWRY P B, et al. 2014.Privacy fa- tigue: the effect of privacy control complexity on consumer elec- tronic information disclosure [J]. Social Science Electronic, Publishing.

8. CHOI H, PARK J, JUNG Y. T 2018.he role of privacy fatigue in on- line privacy behavior [J]. Computers in Human Behavior, 81: 42-51.

9. TANG J, AKRAM U, SHI W. 2020.Why people need privacy? The role of privacy fatigue in App users'intention to disclose priva- cy: based on personality traits [J]. Journal of Enterprise In- formation Management, ahead-of-print (ahead-of- print).

10. OH J, LEE U, LEE K. 2018.Privacy fatigue in the Internet of things environment [J]. It Convergence Practice, 6 (4) :21-34.

11. Palmatier R. W. 2008.Interfirm Relational Drivers of Cus- tomer Value[J].Journal of Marketing, 72(4):76-89.

12. Suh B., Han I..2002. Effect of Trust on Customer Accep- tance of Internet Banking[J].Electronic Commerce Research and Applications, 1(3-4):247-263.

13. Martin K., Borah A., Palmatier R. W. 2017.Data Privacy: Effects on Customer and Firm Performance[J].Journal of Market- ing, 81(1):36–58.

14. Malhotra N. K., Kim S. S., et al. 2004, Internet Users' In- formation Privacy Concerns (IUIPC): the Construct, the Scale, and A Causal Model[J].Information Systems Research, 15 (4): 336-355.

15. Carver C. S., Scheier M. F., Weintraub J. K. 1989.Assessing Coping Strategies:A Theoretically Based Approach[J].Journal of Personality and Social Psychology, 56(2):267-283.

16. Havlena W. J., Desarbo W. S. On the Measurement of Perceived Consumer Risk [J].Decision Sciences, 1991, 22 (4): 927-939.