Research on Influencing Factors and Configuration Paths of Privacy Fatigue of Social Media Users

Lijuan Niu(✉)

School of Journalism and Communication, Zhengzhou University, Zhengzhou, China
1520901211@qq.com

Abstract. The attitude of users towards privacy issues is an important prerequisite for Internet information security governance. Exploring the influencing factors and configuration paths of privacy fatigue will help researchers understand users' privacy protection attitudes, provide management inspiration for network service providers and policy makers, so as to promote the construction of a safe Internet environment. Based on the 303 sample data collected by the questionnaire, we use the fuzzy-set Qualitative Comparative Analysis (fsQCA) to explore the influencing factors and configuration paths of privacy fatigue from the perspective of protection motivation. The results of the study show that there are three conditional configurations that can explain the factors affecting privacy fatigue. Among them, perceived vulnerability and perceived severity are the core conditions that lead to privacy fatigue, while the lack of self efficacy, response efficacy and privacy concern can stimulate the generation of users' privacy fatigue attitude. The study focuses on the perspective of protection motivation to explore the influencing factors of privacy fatigue of social media users, and provides a new interpretation angle for privacy fatigue research.

Keywords: social media · privacy fatigue · Protection Motivation Theory · fsQCA

1 Introduction

With the deep embedding of the network into people's lives, social media applications based on mobile terminals have also caused a series of privacy and security issues while enriching people's daily lives. Due to the characteristics of fast information dissemination, multiple infringing subjects, and serious infringement consequences, social media has become a hardest hit area for cross-border acquisition of user privacy. However, despite the endless emergence of social media privacy leaks, people's attitudes and ways of dealing with privacy issues seem to have quietly changed with the continuous penetration of technology, and a feeling of burnout about online privacy issues has begun to spread among the crowd. According to a survey of Internet consumers by Kaspersky Lab, 56% of users believe that it is impossible to protect personal privacy on the Internet, 32.3% of users do not know how to protect their online privacy, 18.1% of users express

G. Ali et al. (Eds.): ISEMSS 2022, ASSEHR 687, pp. 2355–2364, 2022.
https://doi.org/10.2991/978-2-494069-31-2_277

willingness to trade privacy for free services [1]. This inability to deal with privacy issues often leads people to ignore the potential risks and excessively transfer personal privacy information on social networks, which makes personal privacy face severe challenges. Under the penetration of big data algorithm technology, people tend to shift from passive privacy transfer to active privacy disclosure in pursuit of a better network service experience, which not only provides an opportunity for criminals to obtain personal privacy, but also seriously hinders the healthy development of the Internet industry. In this context, the study attempts to answer the following questions: What factors might influence privacy fatigue among social media users? How do these factors relate to each other and contribute to privacy fatigue?

2 Theoretical Background

2.1 Privacy Fatigue

Privacy fatigue reflects a useless state of mind that users may develop when considering their privacy. Users believe that there is no effective way to manage their personal information on the Internet, so they "turning a blind eye" to privacy issues. At present, scholars at home and abroad have carried out relevant research on the phenomenon of privacy fatigue. Overall, the research shows two characteristics: One is that some scholars use empirical research to introduce privacy fatigue as a theoretical tool or perspective to investigate the results of privacy behavior [2, 3], the other is mainly to analyze social e-commerce users or broader Internet users as the research object [4–6]. Since privacy fatigue is a relatively new concept, there are few academic research on privacy fatigue, and the domestic research on privacy fatigue is still in the preliminary stage, lacking of systematic research on privacy fatigue. In view of this, we take privacy fatigue as the main concept and use the fuzzy-set Qualitative Comparative Analysis (fsQCA) to try to reveal the complex mechanism of multiple factors acting together on the privacy fatigue of social media users.

2.2 Privacy Concern

Privacy concern is a core concept in the field of privacy management. It is an individual's subjective perception of the social situation in which they live. It describes the individual's level of concern about the illegal collection, acquisition, monitoring, and storage of private information. At present, the research results on privacy concern are quite rich. Many scholars have discussed the relationship between privacy concern and privacy behavior intention, and pointed out that users who are more concerned about personal privacy tend to take privacy protection measures. Privacy concern emphasizes the importance individuals attach to privacy information, while privacy fatigue reflects the indifference of individuals to privacy issues. Therefore, we believe that users with low privacy concern are more likely to suffer from fatigue.

2.3 Protection Motivation Theory

The protection motivation theory was proposed by Rogers in 1975, which explains the process of individuals' behavior change through threat appraisal and coping appraisal in the cognitively mediated process [7]. Specifically, the theoretical framework mainly includes three parts: information source, cognitive mediation process, and coping mode. The cognitive mediation process, as a core component, mainly includes threat appraisal (perceived vulnerability, perceived severity) and coping appraisal (self efficacy, response efficacy). Perceived vulnerability refers to the main belief formed by an individual's subjective judgment on the possibility of experiencing certain negative consequences. Perceived severity refers to an individual's judgment on the degree of threat posed by risk factors to his own interests. Self efficacy refers to an individual's belief in the ability to exercise control over oneself to take certain protective behavior. In other words, the greater the self efficacy, the greater the likelihood of behavioral change. Response efficacy refers to an individual's perception of whether a certain protective behavior is effective. In general, the more individuals believe that they can benefit from the behavior they take, the more motivated they are to take a certain behavior. With the continuous development and improvement of the protection motivation theory, its application scope is gradually expanding. In addition to studying health protection behavior, it has also been applied to the research field of information security behavior. At present, many scholars have used the protection motivation theory to conduct related research on privacy issues, proving the effectiveness of the theory in the social network environment. In the field of information security, protection motivation theory points out the process of individual coping behavior to avoid the risk of privacy leakage or invasion. In view of the fact that the study explores the privacy cognition and protection awareness of social media users from individual factors, which is in line with the theoretical connotation of protection motivation theory, it is suitable as the theoretical basis of the study.

3 Research Design

3.1 Methodology

FsQCA is a theoretical set research method initiated by Ragin. The basic logic of the method is based on the principle of Boolean algebra, by discussing the membership relationship between sets to explore the common characteristics of multiple cases [8]. It focuses on "concurrent causality" across cases, making up for the traditional quantitative research of constant causality, emphasizing the equivalence feature, which means that different combinations of conditions can produce the same results. Therefore, the study innovatively applies fsQCA method to the research of privacy fatigue of social media users to explore the conditional configuration of privacy fatigue.

3.2 Measurement

The measurement of variables is based on previous research and adapted to the context of social media. We used a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The measurement of perceived vulnerability, perceived severity, self efficacy and response efficacy was based on the scale designed by Johnston [9]. Privacy concern was measured using a scale designed by Bansal [10]. Privacy fatigue was measured using a scale designed by Choi [11].

3.3 Sample

The study takes social media users as the research object, and uses snowball sampling method to issue questionnaires through the network platform. We collected a total of 367 questionnaires. After excluding the questionnaires with short answer time, conflicting answers and repeated options, we obtained a total of 303 valid questionnaires. Among the respondents in the survey, there are 125 males, accounting for 41.2%, and 178 females, accounting for 58.7%. In terms of age distribution, respondents aged 20 to 24 accounted for the largest percentage, with a total of 245, accounting for 80.9%. Followed by 38 respondents aged 25 to 29, accounting for 12.5%. The percentages of respondents aged 19 and below, 30 to 34 and 35 and above was 4.0%, 2.3% and 0.3% respectively. In terms of educational background distribution, there are mainly 224 respondents with bachelor's degree, accounting for 73.9%. Followed by 67 respondents with master's degree or above, accounting for 22.1%. Senior high school degree or below, and junior college degree, accounting for 0.3% and 3.6% respectively.

4 Results

4.1 Reliability and Validity Tests

According to Table 1, the composite reliability value of the six variables were all above 0.7, the factor loading coefficients obtained after rotation by principal component analysis were all greater than 0.6, indicating that the scale had good reliability and validity.

4.2 Data Calibration

Calibration is the process of assigning a set membership score to a case. Since the sample is based on the values of five-point Likert scale, and the membership value of fsQCA ranges from 0 to 1, it is necessary to convert the original data into the fuzzy set membership value between 0 and 1. Researchers need to select three qualitative anchors (complete membership, intersection and complete non-membership) based on the existing theoretical knowledge and actual situation, and calibrate the original data through the anchors. Referring to the study of Pappas [12], we set "4" as fully affiliated, "3" as intersection, and "2" as totally non-affiliated, and calibrated the individual variable data.

4.3 Necessary Condition Analysis

It is generally believed that when the consistency is greater than 0.9 [13], the condition can be considered as a necessary condition for the result to occur. We examined the individual necessary conditions of the outcome variables to identify whether the antecedent

Table 1. Results of reliability and validity tests

Variable	Item	Factor loading	CR
Perceived Vulnerability (PV)	PV1	0.873	0.843
	PV2	0.846	
	PV3	0.674	
Perceived Severity (PS)	PS1	0.899	0.879
	PS2	0.890	
	PS3	0.727	
Self Efficacy (SE)	SE1	0.785	0.871
	SE2	0.855	
	SE3	0.856	
Response Efficacy (RE)	RE1	0.721	0.725
	RE2	0.674	
	RE3	0.656	
Privacy Concern (PC)	PC1	0.783	0.867
	PC2	0.853	
	PC3	0.847	
Privacy Fatigue (PF)	PF1	0.730	0.825
	PF2	0.754	
	PF3	0.798	
	PF4	0.657	

conditions and their non-sets are necessary conditions affecting privacy fatigue. Table 2 shows that the consistency of perceived vulnerability and perceived severity is 0.949055 and 0.925394 respectively, indicating that these two factors are necessary conditions and can independently explain the outcome variable of privacy fatigue.

4.4 Truth Table Construction

Truth table is a list of results that categorize all sample data into different combinations. In general, a high frequency threshold is required in samples larger than 150 to remove the combination of consistency or lower frequency. According to Ragin, the frequency threshold should be set to retain at least 75% of the total number of cases and the consistency threshold should not be less than 0.75 [14]. Therefore, we set the frequency threshold to 5 and the consistency threshold to 0.8. In addition, according to the principle that PRI consistency is greater than 0.7 [15], corresponding adjustments are made to the assignment of result variables. The truth table is finally constructed as shown in Table 3.

Table 2. Results of necessity analysis of conditions

Variable	Consistency	Coverage
PV	0.949055	0.718843
~ PV	0.159096	0.727801
PS	0.925394	0.692793
~ PS	0.171544	0.844594
SE	0.566776	0.704930
~ SE	0.582256	0.792362
RE	0.535034	0.707713
~ RE	0.616527	0.787541
PC	0.587533	0.731000
~ PC	0.593109	0.806824

Table 3. Truth table

PV	PS	SE	RE	PC	Sample number	PF
0	0	0	0	0	5	0
1	0	0	0	0	15	1
1	1	1	0	0	22	1
1	1	0	0	1	14	1
1	1	0	1	1	10	1
1	1	0	1	0	13	1
1	1	0	0	0	86	1
0	1	0	0	0	6	0
1	1	1	1	0	16	0
1	1	1	0	1	17	0
0	0	1	0	0	5	0
0	1	1	1	1	10	0
1	0	1	1	1	57	0

4.5 Conditional Configuration Analysis

In the fsQCA analysis, the analysis program will produce three kinds of results: "complex solution", "parsimonious solution" and "intermediate solution". Since the intermediate solution does not eliminate the necessary conditions, the intermediate solution is generally selected in combination with the parsimonious solution to report the results [8]. The conditions that appear in both the intermediate solution and the simple solution

Table 4. Results of conditional configuration

Variable	Configuration		
	1	**2**	**3**
Perceived Vulnerability (PV)	●	●	●
Perceived Severity (PS)	•		•
Self Efficacy (SE)	⊗	⊗	
Response Efficacy (RE)		⊗	⊗
Privacy Concern (PC)		⊗	⊗
Consistency	0.826785	0.868382	0.86869
Unique coverage	0.527426	0.420965	0.462855
Raw coverage	0.127908	0.0214474	0.0633367
Overall solution consistency	0.818368		
Overall solution coverage	0.61221		

are called core conditions, and the conditions that appear only in the intermediate solutions are called peripheral conditions [16]. They all have certain influence on the result. Table 4 reflects the consistency and coverage results for the antecedent configuration of privacy fatigue. The consistency index is to judge the relationship degree of each configuration path constituting a subset of the condition set. The coverage index is to judge the explanatory power of each configuration to the total sample. It can be seen that the consistency and overall consistency of the three configuration paths are higher than the acceptable threshold of 0.75, showing high consistency, indicating that they are all sufficient conditions to cause privacy fatigue. In terms of coverage, the three configuration paths explained 53%, 42%, and 46% of the samples respectively, and the overall coverage reached more than 60%.

5 Disucssion

The study found three configuration paths that lead to privacy fatigue as follows.

Configuration 1: perceived vulnerability * perceived severity * ~ self efficacy → privacy fatigue. In this path, perceived vulnerability and perceived severity are the antecedent conditions leading to privacy fatigue, and self efficacy is the missing core condition. This means that when users lack the ability and belief to protect their privacy, they are prone to burnout if they have a high assessment of privacy threat.

Configuration 2: perceived vulnerability * ~ self efficacy * ~ response efficacy * ~ privacy concern → privacy fatigue. This configuration shows that perceived vulnerability is the core condition leading to privacy fatigue, while self efficacy, response efficacy and privacy concern are all missing conditions. Compared with the first path, this path reflects that some social media users have a certain cognitive bias on privacy issues. Some users think that the measures they take to reduce privacy problems are largely ineffective, so they ignore the potential risks and take a negative attitude to deal with them.

Configuration 3: perceived vulnerability * perceived severity * ~ response efficacy * ~ privacy concern → privacy fatigue. In configuration 3, users with strong perceived vulnerability, lack of response efficacy and lack of privacy concern are more likely to induce privacy fatigue. Some users believe that privacy measures cannot manage personal privacy information well and when individual privacy concern is low, they may avoid privacy issues and be indifferent to them even in the face of a relatively high threat of privacy leakage.

From the analysis of the above conditional configurations, it can be found that the perceived vulnerability is the core condition in the three configuration paths, and the perceived severity is the peripheral condition in the configuration 1 and 3. This reflects that users who are more sensitive and to privacy threat are more likely to feel tired when facing the risk of privacy exposure. The protection motivation theory states that out of self-preservation instinct, individuals will hope to avoid situation where they face threat by changing in some way. In this sense, individuals will be motivated to protect themselves in order to deal with the threat that privacy disclosure may pose to them. However, the study draws a result that contradicts the theoretical direction: users show a burnout-centered avoidance response when faced with privacy threat. This finding explains to a certain extent the phenomenon of "privacy paradox" that exists widely in the network environment. On the one hand, due to the threat of privacy leakage, users tend to strengthen privacy protection. On the other hand, under the influence of privacy fatigue, they tend to be indifferent to privacy issues. Some research have pointed out that perceived threat will significantly increase the privacy fatigue, indicating that perceived threat will make users psychologically stressed and more likely to cause burnout. This finding of the study confirms the conclusions of previous research.

From the analysis results of the conditional configuration, self efficacy is the missing core condition in both configuration 1 and configuration 2, and response efficacy is the missing condition in configuration 2 and configuration 3, which means the lack of privacy protection self efficacy and response efficacy users are more likely to suffer from burnout. This conclusion is consistent with the hypothesis mentioned in the protection motivation theory that the demand for personal information privacy protection can be improved through perceived efficacy. According to the protection motivation theory, self efficacy and response efficacy, as important variables in the process of coping appraisal, describe the ability of individuals to expect to reduce threats by adopting a certain coping patterns. They play an important role in restraining the formation of privacy fatigue. Therefore, for users, enhancing privacy protection awareness and improving privacy literacy can help to restrain burnout.

In addition, the variable of privacy concern is the missing condition in both configuration 2 and configuration 3, indicating that users who are more concerned about privacy issues are more cautious when facing privacy issues, so it is not easy to cause burnout. In social media privacy research, privacy concern has always been regarded as an important variable affecting users' privacy attitude and behavior. The results of the study suggest that the privacy concern play a key role in the pathway that act on the attitude of privacy fatigue. Therefore, we should take privacy concern seriously. On the one hand, social media platforms should control the reasonable privacy boundary and try their best to help users reduce their concern in the process of using, such as regularly checking website security vulnerabilities and strengthening supervision. On the other hand, relevant policy makers should strengthen the popularization and training of network security knowledge, guide users to pay attention to privacy policies and laws, which will also help to reduce their negative feelings.

6 Conclusions

We collected data through a questionnaire survey, and used the fsQCA method to explore the influencing factors and configuration paths of privacy fatigue of social media users from the perspective of protection motivation. In this paper, we found that there are three conditional configurations that can explain the influencing factors of privacy fatigue of social media users. Among them, perceived vulnerability and perceived severity are the core conditions that lead to privacy fatigue, while the lack of self efficacy, response efficacy and privacy concern can stimulate the generation of users' privacy fatigue attitude.

6.1 Implications

The contributions of the study are as follows: firstly, we try to use the fsQCA method to explore the multiple concurrent factors of privacy fatigue of social media users. It breaks through the limitation of previous quantitative research focusing on constant causality. Secondly, the study focuses on the perspective of protection motivation. It is found that the threat appraisal, coping appraisal and privacy concern of users to privacy can act on the privacy fatigue of social media users in different configuration paths. This discovery could also help future researchers to better understand the mechanism of privacy fatigue.

6.2 Limitations

The study still has the following limitations. Firstly, there are too many types of social media at present, and the operating mechanisms of social media with different attributes are also different, which is not distinguished in our research. The next step is to try to compare and analyze the difference of the results of different platforms. Secondly, we mainly discuss the influencing factors of privacy fatigue of social media users from the perspective of personal factors, while other external factors such as platform and environment that may also be important causes of privacy fatigue. Therefore, the influence path of external factors and their combination can be paid more attention in the future.

References

1. Kaspersky daily. The true value of digital privacy: are consumers selling themselves short? https://www.kaspersky.com/blog/privacy-report-2019/.
2. JIANG Ling, WANG Zhihua, YANG Guoliang. Research on the Influence Mechanism of Consumers' Personal Information Disclosure in Network Context——Based on the Theoretical Perspective of Privacy Fatigue. Enterprise Economy. Vol. 39 (2020) No. 9, p. 80-87.

3. WU Chake. Influencing factors of social media user’s willingness of privacy disclosure from privacy fatigue perspective. The degree of Master, Tianjin Normal University, China, 2019.
4. WU Dingjuan, ZHU Hou. The formation mechanism of consumer privacy paradox in online shopping under dual attitude. Journal of Intelligence. Vol. 39 (2020) No. 8, p. 160-165+173.
5. XU Yiming, LI He, YU Lu. Research on the influence of self-efficacy of privacy protection on privacy behaviors of social network users. Library and Information Service. Vol. 63 (2019) No. 17, p.128-136.
6. ZHANG Dawei, XIE Xingzheng. Empirical research on the drivers of digital native’ intention to protect privacy: The moderating role of privacy fatigue. Information studies: Theory&Application. Vol. 44 (2021) No.7, p. 101-110.
7. WANG Yun, XIAO Xia, ZHENG Pinpin, et al. Application and development of protection motivation theory in individual behavior change. Chinese Journal of Health Education. Vol. 25 (2009) No. 11, p. 853-870.
8. ZHANG Ming, DU Yunzhou. Qualitative Comparative Analysis (QCA) in Management and Organization Research:Position, Tactics, and Directions. Chinese Journal of Management. Vol. 16 (2019) No. 9, p. 1312-1323.
9. Johnston A C , Warkentin R . Fear appeals and information security behaviors: An empirical study. Mis Quarterly, Vol. 34 (2010) No. 3, p. 549-566.
10. Bansal G , Zahedi F ’ , Gefen D . The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems, Vol. 49 (2010) No. 2, p. 138-150.
11. Choi H , Park J , Jung Y . The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81.APR.(2018):42-51.
12. Pappas I O , Woodside A G . Fuzzy-set Qualitative Comparative Analysis (fsQCA): Guidelines for research practice in Information Systems and marketing. International Journal of Information Management, Vol. 58 (2021) No. 3, p. 1-23.
13. Ragin C C . Fuzzy-set Social Science. University of Chicago Press, 2000.
14. Ragin C C , Strand S I , Rubinson C . User’s guide to Fuzzy-Set/Qualitative Comparative Analysis. University of Arizona. Vol. 3 (2008) No. 9, p. 87-101.
15. Greckhamer T , Furnari S , Fiss P C , et al. Studying configurations with qualitative comparative analysis: Best practices in strategy and organization research. Strategic Organization, Vol. 16 (2018) No. 4, p. 482-495.
16. DU Yunzhou, JIA Liangding. Configuration perspective and qualitative comparative analysis (QCA): a new way of management research. Management World, (2017) No. 6, p. 155-167.