Development and Construction of a User Privacy Concern Measurement Scale in Social Media

Runting Li[1(✉)] and Yuan Wang[2]

[1] Journalism Department, Guangzhou Huashang College, Guangdong 511300, China
runtingli1022@gmail.com
[2] Foreign Language Department, Guangzhou Huashang College, Guangdong 511300, China

Abstract. The concept of privacy concerns was first proposed in the research of e-commerce content, so the concept is not native to the social media environment. Therefore, the primary problem to be solved in this study is to explore new issues of privacy concerns in the current social media environment through literature review and expert interviews, sort out the privacy concern measurement dimensions suitable for social media, and form a measurement scale for privacy concerns in social media.

Keywords: Social media · Privacy concerns · Measurement scale

1 Introduction

With the deepening of privacy research, the measurement of public attitudes towards privacy has become an urgent problem to be solved. In this regard, scholars in the field of Western management took the lead in putting forward the concept of "information privacy concerns" to measure the public's attitude towards privacy [1].

The research on privacy concerns began in the field of e-commerce. After the measurement scale gradually matured, the research expanded to the field of social media. In the early stage of privacy concerns research, the commonly used implicit measurement scale was GIPC [2], also known as the one-dimensional global information privacy concern measurement scale, but this scale is only a preliminary design and cannot accurately reveal the specific situation of consumers' privacy concerns. With the needs of research and development, in order to better understand privacy concerns and obtain data on personal concerns about information privacy practices through scientific measurement, Smith and other scholars (1996) have tried to develop a multi-dimensional scale of information privacy concerns, namely CFIP scale. The content of the scale includes collection, misuse and illegal use, and unauthorized secondary use. There are 15 items to measure these four aspects, so that users' information privacy concerns can be measured in a more detailed and accurate way. The validity of these 15 items has also been confirmed by scholars such as Stewart and Segars (2004) in an empirical study of psychometric properties [3]. Malhotra et al. (2004) designed the Internet Consumer Information Privacy Concern Scale (IUIPC for short), which includes three dimensions: collection, control, and perception of privacy practices [4]. Rifon et al.

(2005) [5] proposed a scale, which is applicable to exploring the relationship between privacy issues and subsequent behaviors through one-dimensional measurement. Mei (2003) [6] found that Internet users' privacy concerns, as a second-order form factor, include three first-order dimensions: collecting, controlling and understanding. Dinev and Hart (2005) argue that privacy mainly includes four aspects: notification, access, choice, and security [7].

2   Literature Review of Measurement Scales

2.1   Feasibility Analysis of IUIPC Scale

Under the research of Western scholars, the privacy scale has gradually matured, which has also attracted the attention of domestic scholars. Yang, Wang, and Wang (2005) believed that the IUIPC scale is more suitable for testing in the Chinese context [8]. Chinese scholar Shen (2013) used the three dimensions of the IUIPC scale for the first time to examine netizens' concerns about online information privacy in general online behavior. Shen's research proved the rationality and effectiveness of expanding the research scope of IUIPC scale to a certain extent. Specifically, when analyzing online privacy issues, we can try to adopt the IUIPC scale in the study of online information privacy issues. However, at the same time, this study is based on secondary data analysis, so the construction, reliability and validity of the scale need to be further improved. This study takes college students as the research object, which also has certain limitations. After that, Qi (2018) analyzed the privacy concerns of the Chinese public and their influencing factors in the context of big data by referring to the research results of the IUIPC scale. The results further confirmed the applicability of the IUIPC scale in China.

2.2   Research Status of Privacy Concerns and Social Media

With the development of media technology, social media has gradually emerged and embedded into people's daily life. The privacy concerns of social media have gradually attracted the attention of some scholars, who have started to conduct in-depth research. After sorting out the literature in this area, the main research can be divided into several streams as the following.

First of all, the first kind of research is guided by the research tradition and combined with the existing basic theoretical model to explore the privacy concern For example, Tan et al. (2012) [9] used the data of users of social networking sites to conduct research and analysis in combination with the Technology Acceptance Model (TAM), and explained that there is no direct causal relationship between privacy issues and users' willingness to adopt, but more is a correlation. At the same time, they also pointed out that the moderating effect of privacy concerns on users' continued use of social media, which can affect users' perceived usefulness and perceived ease of use. Also based on the privacy computing theory in TAM, Zhang (2017) [10] studied the "privacy paradox" of social media in the Chinese context in combination with the privacy boundary theory. In subsequent research, she also explored the formation mechanism of privacy concerns of social media users. Starting from the theory of technology acceptance, Liu (2016)

[11] focused on privacy concerns, conducted a systematic study with the intention of personal privacy disclosure as the mediating variable, and established a research model of social media technology acceptance and function acceptance behavior. The research of these scholars has provided a solid theoretical basis and frame reference for future in-depth research.

Second, some studies are based on privacy concerns, enriching the research content of each dimension of privacy concerns from different directions. For example, Guo (2013) [12] focused on the dynamics of privacy concerns caused by factors and privacy concerns and established a dynamic influence model. Specifically, in the research, he took Weibo as the research object, mined its characteristics as a social networking site, and introduced the perceived benefit variable into the dynamic model to study the influence of this variable on user behavior.

Third, some studies on social media privacy concerns are more detailed in terms of research objects. For example Feng (2014) [9] focused on the impact of privacy concerns on adolescents' privacy-protecting behaviors in social networking sites. Through the classification of the above studies, it can be found that privacy concerns and social media are gradually intertwined, and privacy concerns are affected by many different factors in the social media environment, and new changes have taken place. Relevant research elements are not limited to the dimensions of IUIPC scale.

By combing the literature related to privacy concerns, it is found that most of the current research on privacy concerns has adopted the IUIPC scale. Although the scale is relatively mature, its update speed has not kept up with that of social media. Especially in the environment of rapid technological change, new privacy problems of users occur frequently, and the privacy paradox problem is still acute. Future research urgently needs to re-examine the IUIPC scale to explore its applicability in the current social media environment, and whether it needs to be updated and supplemented, in order to better explain the current privacy paradox and other issues.

3   Dimensional Exploration of Privacy Concerns Measurement Scales

Privacy concerns are used to describe individuals' subjective feelings about privacy status, and are the core factors that can measure users' privacy issues and risk assessments. This subjective feeling includes the illegal collection, detection, acquisition, transmission and storage of users' private information [13].From the previous literature review, it can be concluded that most of the current studies on privacy concerns use the IUIPC scale, and through empirical tests, all dimensions of the IUIPC scale have been confirmed that it is more suitable for the Chinese background than other scales. Therefore, this study mainly draws on the three dimensions of perception, control and collection in the IUIPC scale. However, as Smith (1996) said, "dimensions are neither absolute nor static, because advocates, consumers and scholars perceptions may change over time." Especially with the continuous updating of the current social media privacy communication environment, such as the emergence of personalized push, user portrait, community operation and other user management methods, the personal information in the platform is no longer simply used on one hand, but more collected through collection, sorting

and analysis for "secondary use" on the other. The degree of users' perception of the secondary use of personal information on social media platforms has not been scientifically measured. Therefore, this research focuses on testing the perception of second use into the dimension of privacy concerns, and examines the user's perception of the secondary use of personal privacy as one of the research dimensions of social media privacy concerns.

3.1 Collection

Collection is defined as the extent of a person's relationship to the value gained by others, and the act of collecting data, whether legal or illegal, is the starting point for a variety of information privacy issues. The collection factor is proposed based on the principle of distributional fairness in Rousseau's (1778) social contract theory. The collection dimension in IUIPC scale is a continuation of the CFIP scale's definition of collection. Therefore, the collection factor captures the central theme of the fair exchange of information based on an agreed social contract, which involves "the perceived fairness of the outcomes one receives" (Culnan and Bies 2003, p. 328). In a fair exchange, consumers give up some information in exchange for something valuable after evaluating the costs and benefits associated with a particular transaction. Therefore, if individuals expect negative results in the use of social media, they will not be willing to disclose their personal information (Cohen 1987). Whether the value is equal is the standard to measure the collection. How individuals measure the value of their personal information depends on the value they can obtain when collecting it. If it is equal, the concern for privacy may be reduced, so the value balance is the collection dimension to measure privacy concerns.

3.2 Control

Individuals often take great risks when disclosing themselves on social media, so the control of privacy has become an important dimension of privacy concerns. The logic that an individual would consider the procedure to be fair is presented. In other words, when exchanging or self-disclose information, social media users often want to control the scope of information dissemination, and even the recipients of information. At the same time, control is an active control over information privacy, which is usually achieved by approving, modifying, and choosing to join or exit opportunities. When individuals perceive that they cannot control the results of the dissemination, they will choose to refuse to spread private information to the outside world. Therefore, the control factor also represents the freedom of individuals to disclose or opt out of private information on social media.

However, it is worth mentioning that when there is a greater possibility of opportunistic behavior and violation of social contract in relationship exchange, the problem of control becomes prominent. And privacy-infringing platforms or individuals are on the rise, and they often break contracts for profit motive, thus pushing the privacy issue to the front. Therefore, the core issue of privacy concerns in current social media lies in whether social media users' control over their privacy can be presented in a practical

way. This study believes that control is an important variable that reflects the dimension of social media users' privacy concerns.

3.3 Perception

Compared with control and collection, the perceived privacy concern dimension is a passive dimension of information privacy, which refers to the degree to which social media users pay attention to their organization's information privacy practices (Culnan 1995; Foxman and Kilcoyne 1993). Control means that users actively control private information, while perception is relatively passive. Perceived factors include interactive justice and information justice. Specifically, in the social media environment, interactive justice refers to the priority and transparency of information dissemination in the process of private information dissemination. At the same time, information justice in social media refers to the specific information disclosed by users. When users know the specific information of justice information, their perception of fairness can be enhanced (Malhotra et al. 2004). Generally speaking, the perception dimension emphasizes the user's perception of the information collected or disclosed. This study includes this dimension to examine the impact of perception on privacy concerns in social media.

3.4 Secondary Use

The concept of "secondary use" is relative to the concept of "single use". The concept of "single use" refers to the directness the data acquisition process. The subjects of information acquisition include individuals and organizations, such as the information that the user needs to enter when logging in for the first time or purchasing a product. "Secondary use" refers to processing, analyzing and processing the obtained data, and then using the obtained modified data. For example, the platform can form more accurate user privacy information through data analysis of data obtained by users after browsing. However, in the privacy ownership principle, people believe that their private information belongs to them. Even after granting others the right to know their information, the original owner of the information still believes that they are the only owner of the information (Petronio and Gaff 2010). In other words, from a behavioral perspective, people perceive themselves as owning their private information in the same way that they own other property (Child and Petronio 2011; Child et al. 2009). They can lend to others, but they still believe that the property is still theirs.

Smith (1996) [2] considered that the limitation of technology and the pressure from secondary use are not easy to be detected. However, with the development of technology, especially the overlap between the current era of big data and social media, the concept of personal privacy information has been repeatedly refreshed. Now it can be considered that users are on the Internet. Any data generated during use can be considered as personal private information. However, there is still a relative lack of awareness of the secondary use of privacy in the new environment. Therefore, this study hopes to emphasize the important role of secondary use in the current environment by incorporating the dimension of secondary use into the dimension of privacy concerns.

4   Social Media Privacy Concern Measurement Scale Measurement

On the basis of previous studies, this study draws on the three dimensions of the IUIPC scale of Malhotra (2004): control, collection and awareness, while taking the current social media personalized push and user portraits into account. With the emergence of user management methods, such as community operation, personal information is no longer a simple first-hand use on the platform, but rather "secondary use" through collection, sorting and analysis. Therefore, in the Structured Privacy Concerns Inventory (CFIP), Smith et al. proposed the secondary use in privacy problem measurement for the first time. This dimension has been proposed and generally recognized by the academic community.

The privacy concern measurement scale in this study is based on the IUIPC scale with the "secondary use" dimension to measure. Finally, four dimensions and 12 items are determined. In order to better design and develop the scale, it is necessary to discuss its reliability separately to better carry out formal measurement. Cronbach's alpha coefficient was used to test the reliability of the questionnaire in this study. The following is the detailed process for calculating the reliability of the scale.

On the basis of the previous small sample survey, the Privacy Concern Measurement Scale, the Privacy Rule Establishment Measurement Scale and the Boundary Management Measurement Scale were adjusted, and the scales were verified by large sample test. The large sample detection of this study was concentrated in February 2020 with two groups of data collected online. 390 questionnaires were collected for the first time, and 155 questionnaires were collected for the second time. The respondents were mainly from Guangdong, Beijing, Zhejiang, Shandong and other places, and a total of 545 questionnaires were collected.

4.1   Reliability Analysis of Privacy Concern Measurement Scale

Table 1 shows the reliability coefficient table of the four dimensions of collection, control, perception and secondary use in privacy concerns. As can be seen from Table 1, Cronbach's α coefficients are all greater than 0.8, which indicates that each measurement item of the privacy measurement scale has good reliability, stability and consistency in the scale, and meets the requirements of statistical analysis.

4.2   Validity Analysis of Privacy Concerns Measurement Scale

In the large-sample phase of privacy concerns measurement, the KMO test coefficient is 0.829, indicating that it is suitable for factor analysis. At the same time, 12 measurement items are categorized into four dimensions, and their contribution rate (explaining strength) is 77.746%, which has strong explanatory power. It can be seen from the table that in the validity analysis of large samples, the eigenvalues of the factors extracted from the privacy concern measurement scale data are quite different, so it can be preliminarily considered that the extracted factors can explain the factors detected in the large sample detection. Most of the variables of this privacy concern measurement scale can then be generalized and analyzed.

Table 1. Reliability Analysis of Privacy Concern Measurement Scale

Dimension	Measurement item	Cronbach's α
Collection	3	0.850
Control	3	0.851
Perception	3	0.848
Secondary Use	3	0.852

Table 2. KMO and Bartlett's Tests for Privacy Concern Measurement Scales

KMO Sampling Suitability Quantity		.829
Bartlett's sphericity test	Approximate chi-square	3838.144
	degrees of freedom	66
	Significance	.000

4.3 Factor Analysis of Privacy Concern Measurement Scale

The reliability coefficient table of the four dimensions of collection, control, perception and secondary use in privacy concerns is shown in Table 1. It can be seen from the table that Cronbach's α coefficients are all greater than 0.8, and it can be considered that each measurement item of the privacy measurement scale It has good reliability, stability and consistency in the scale, and meets the requirements of statistical analysis.

In terms of validity, it can be seen from Tables 2 and 3 that the KMO test coefficient is 0.829 in the measurement of privacy concerns in the large sample stage, indicating that factor analysis is suitable. It is 77.746%, which has a relatively strong explanatory power. It can be seen from the table that in the validity analysis of large samples, the difference between the eigenvalues of the factors extracted from the data of the privacy concern measurement scale is relatively large, and it can be preliminarily considered that the extracted factors can explain the detected factors in the large sample detection. Most of the variables of this privacy concern measurement scale can then be generalized and analyzed.

On the basis of the KMO and Bartlett's sphericity test in the privacy concern questionnaire, the principal component analysis method was used to conduct exploratory factor analysis on all the questions in the questionnaire, and the fixed number of factors was set to 4, that the definitions of these measurement items are clear, and this scale can well measure variables (Table 4).

5   Conclusion

Most of the elements in the current privacy concerns measurement scale come from the Internet Consumer Information Privacy Concern Scale (IUIPC) designed by Malhotra et al. (2004) using social contract theory. The scale includes three elements: collection,

Table 3. Principal Component Analysis for Large Sample Test of Privacy Concern Measurement Scale

Components	Initial eigenvalues			Rotational Loading Sum of Squares					
			Cumulative %	total	percent variance	Cumulative %	total	percent variance	Cumulative %
1	5.915	49.293	49.293	5.915	49.293	49.293	2.357	19.639	19.639
2	1.255	10.457	59.750	1.255	10.457	59.750	2.344	19.530	39.169
3	1.168	9.732	69.482	1.168	9.732	69.482	2.331	19.423	58.592
4	.992	8.264	77.746	.992	8.264	77.746	2.298	19.154	77.746

Table 4. Factor analysis results of privacy-concerned large-sample validation

	Element			
	1	2	3	4
Control 1	.782			
Control 2	.907			
Control 3	.754			
Collect 1		.768		
Collect 2		.902		
Collect 3		.754		
Secondary use 1			.749	
Secondary use 2			.889	
Secondary use 3			.769	
Perception 1				.710
Perception 2				.897
Perception 3				.781

control and perception of privacy practices. However, since the measurement table is based on e-commerce and different from the current social media, it is planned to focus on the current social media environment. This paper suggests to excavate the changes in the content and depth of users' privacy concerns in the environment, as well as the new factors affecting privacy concerns in the new media environment, and verified, improved and updated the mature IUIPC scale.

References

1. Kerlinger F. Foundations of Behavioral Research. New York: Holt, Rinehart and Winston, 1984: 212-220.
2. Smith H J, Milberg S J, Burke S J. Information Privacy: measuring individuals' concerns about organizational practices [J]. MIS Quarterly, 1996, 20(2): 167-196
3. Stewart K A, Segars A H. An empirical examination of the concern for information privacy instrument [J]. Information Systems Research, 2002, 13(1): 36-49.
4. Malhotra N K, Kim S S, Agarwal J. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model [J]. Information Systems Research, 2004, 15 (4): 336-355.

5. Rifon N J. LaRose R., Choi S M. Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures[J]. Journal of Consumer Affairs, 2005, 39 (2):339-362

6. Mei Shaozu. Network and Privacy [M]. Qingping Humanities Press, 2003.

7. Dinev T, Hart P. Internet Privacy Concerns & Social Awareness as Determinants of Intention to Transact [J]. International Journal of Electronic Commerce, 2005,10(2):7-29.

8. Yang Shu, Wang Yuan, & Wang Kanliang. Research on the Privacy Concern Scale for Chinese Consumers in the Internet Environment. Journal of Intelligence. 27(10), 2005.

9. Y. Feng, W. Xie. Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. Computers in Human Behavior, 2014, 04 (33):153~162

10. Zhang Huiping, Yang Jingdian, Tang Zhiwei. Research on the formation mechanism of social media user information privacy concerns [J].

11. Liu Jiqun. Research on the heterogeneity of social media function acceptance from the perspective of user privacy concerns [J]. Library Forum, 2016(11):16-26

12. Guo Longfei. Research on the dynamic influencing factors and behavioral laws of social network users' privacy concerns: [PhD dissertation]. Beijing: Beijing University of Posts and Telecommunications, 2013.

13. Hanus B, Wu Y. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective [J]. Information Systems Management, 2016, 33(1):2-16.