Research on the Influencing Factors of User Privacy Disclosure Behavior Based on DEMATEL Model

Jinglei Li

Dalian University of Technology School of Economics and Management, Dalian, 116024

Email: stella_jingleilee@163.com

Abstract. [Purpose/Significance] In order to deeply understand the user privacy disclosure behavior in the big data environment, so as to effectively formulate privacy protection strategies and promote sustainable digital development. **[Methods/Process]** This study followed the system thinking and built an index system of influencing factors of user privacy disclosure based on the four dimensions of ELM model. We used the Dematel method to quantitatively evaluate the indicators and identify eight important factors. **[Results/Discovery]** Through comprehensive analysis, this study reveals the factors that have been confirmed by previous studies, such as trust, perceived privacy risk and perceived fairness. Moreover, it finds the factors that have not been fully paid attention to by the academic community, such as cognitive needs, user personality traits, emotional value and reputation, providing a new perspective and theoretical basis for the study of user privacy disclosure. **[Value]** Based on the research conclusion, this paper suggests: analyze user privacy sensitivity to ensure user retention; Improve interaction strategies and cultivate emotional value; Improve privacy policies and enhance perceived fairness.

Keywords: Dematel model; privacy disclosure; Elaboration likelihood model

1 Introduction

In the age of big data, the fusion of old industries and internet technology has given rise to new firms like e-commerce, social networking, and IoT. These services run on the personal data that has become essential resources. Consumers consent to data collecting for convenience, but the use of mobile devices and the sharing of information raises privacy and security concerns. Incidents like data breaches and illicit record sales have increased user awareness. According to the *Mobile Application Security Situation Analysis Report 2020*[1], 58.88% of apps still have security flaws like collecting personal information despite explicit user refusal, which includes cases of forced data collection, privacy violations, and unauthoritative selling of user records. The complexity of the factors causing privacy disclosure makes protection difficult. For data sharing and user trust, it is essential to identify these elements. To overcome this issue, industry and academics must work together.

X. Ding et al. (eds.), *Proceedings of the 2023 4th International Conference on Big Data and Social Sciences (ICBDSS 2023)*, Atlantis Highlights in Social Sciences, Education and Humanities 12,
https://doi.org/10.2991/978-94-6463-276-7_32

2 Literature Review

Privacy Disclosure refers to the act of users voluntarily sharing personal information, which is typically information that they would keep private and undisclosed. Researchers have studied a variety of situations, including social media, e-commerce, and online medical groups.

In online health communities, five main categories of factors influence users' privacy disclosure. These include subjective differences[2], trust[3], service effectiveness[4], emotional value[5], health conditions, and social influences. Conversely, users in social media settings emphasize personalized services and content quality. Emotional factors such as habits, trust, attachment, and fairness also play vital roles in social media due to emotional value. Moreover, e-commerce factors are influenced by privacy invasion impact and privacy indifference.

Based on the aforementioned theoretical foundation, scholars have constructed research models combining theories such as privacy calculation theory, social exchange theory, social capital theory and attachment theory. They have employed methods like regression analysis, structural equation modeling, polynomial regression, response surface analysis, and qualitative research to verify factors influencing privacy disclosure. As the Internet and big data advance, game theory and machine learning gain attention. However, current research often confines analysis, limiting comprehensive assessment of these factors. Additionally, few studies applied decision theory in this field. The article aims to comprehensively consider factors, employ the Dematel method for quantitative assessment, identify key factors, and propose improvement suggestions for privacy protection strategies.

3 Research Design

The Elaboration Likelihood Model (ELM) is based on the dual-process model of human cognition [6]. ELM posits that attitudes can be changed through two routes: the central route and the peripheral route. The central route involves high cognitive effort processes that engage concepts, logic, and rational thinking, while the peripheral route requires lower cognitive effort, relying more on feelings, experiences, and beliefs[7].

Table 1. Indicator System of User Privacy Disclosure Based on ELM Model

Dimension	Code	Influencing Factor	References
Central Path Factors	E1-2	Perceived usefulness, Ease of use	Zhu G[8]
	E3-4	Material Incentives, Personalized services	Wang Y.C[4]
	E5-6	Privacy Risk, Subjective Norms	XU H[9]
	E7	Perceived Fairness	Culnan[10]
Peripheral Path Factors	E8-9	Procedure Fairness, Privacy Policy	Wirtz J[11]
	E10-11	System Quality, Level of Regulation	Han P[12] Ilhan A[13]

	E12	Reputation	KIM D J[14]
Motivation	E13-14	Cognitive need, User personality traits	Aharony N[15]
	E15-16	Trust, Norm of Reciprocity	NieY.H[16]
	E17	Emotional Value	Qiu J.P[5]
Capacity	E18-19	Privacy control ability, Privacy awareness	Guo Y[17]

Existing research has verified the effectiveness of the dual-route model of ELM in user health privacy disclosure behavior[18]. Moreover, according to ELM theory, the specific route a user chooses depends on their motivation and ability[19].Factors like professional knowledge and involvement, cognitive demands, work relevance, and concern for information privacy have been verified to have moderating effects in influencing attitude change and behavioral intent. Table 1 presents the indicator system.

4 Key Factors Identification of User Privacy Disclosure Behavior based on DEMATEL Model

4.1 Constructing and Computing the DEMATEL Model

Construction of the Normative Influence Matrix.

First, the expert group was invited to judge the logical relationships between the influencing factors of user privacy disclosure based on their professional knowledge and research experience. They conducted pairwise comparisons of the logical relationships between each factor and assigned scores according to the degree of influence. This resulted in 15 direct influence matrices A.

Using the row-sum and maximum-value method, each direct influence matrix was normalized to obtain 15 standardized direct influence matrices B. The transformation formula is as shown in Equation (1).

$$B = \frac{A}{\max\limits_{1 \le i \le 19} \sum_{j=1}^{19} a_{ij}} \tag{1}$$

After calculating the average of the 15 standardized direct influence matrices, the normative influence matrix Y was obtained.

Construction of the Comprehensive Influence Matrix.

After obtaining the standardized influence matrix Y, in order to further identify key influencing factors, the comprehensive influence matrix T was calculated according to Equation (2). The elements in matrix T indicate the comprehensive influence degree of factor E_i on factor E_j.

$$T = B(I - B)^{-1} \tag{2}$$

Identification of Key Influencing Factors

Summing up the elements of each row in the comprehensive influence matrix yields the influence degree (D), while summing up the elements of each column yields the influenced degree (C). Adding up the influence degree, affected degree, causality, and centrality yields S. Factors with S value higher than average are identified as key influencing factors. Findings are summarized in Table 2.

Table 2. Identification of key influencing factors

Code	Influence Degree D	Influenced Degree C	Centrality D+C	Causality D-C	Comprehensive Influence Value S	Key Influencing Factor
E1	1.773	2.089	3.862	-0.316	7.408	×
E2	1.531	1.632	3.164	-0.101	6.226	×
E3	1.641	0.764	2.405	0.877	5.687	×
E4	2.045	1.334	3.379	0.711	7.469	×
E5	1.813	2.811	4.625	-0.998	8.251	√
E6	1.875	1.981	3.856	-0.106	7.606	×
E7	1.787	2.721	4.508	-0.934	8.082	√
E8	1.969	1.530	3.500	0.439	7.438	×
E9	2.014	1.548	3.561	0.466	7.589	×
E10	1.905	1.866	3.770	0.039	7.58	×
E11	2.001	1.526	3.528	0.475	7.53	×
E12	2.043	2.241	4.284	-0.198	8.37	√
E13	2.364	1.527	3.891	0.837	8.619	√
E14	2.315	1.014	3.329	1.301	7.959	√
E15	2.108	3.180	5.287	-1.072	9.503	√
E16	1.484	2.570	4.054	-1.086	7.022	×
E17	1.829	2.463	4.292	-0.633	7.951	√
E18	1.857	1.874	3.730	-0.017	7.444	×
E19	2.093	1.777	3.870	0.316	8.056	√

4.2 Result Analysis

Centrality Analysis

The top-ranked factors are trust, perceived privacy risk, perceived fairness, emotional value, reputation, reciprocity norm, cognitive needs, privacy awareness, perceived usefulness, and subjective norm. This suggests users consider privacy disclosure carefully, influenced by emotional value. Notably, perceived privacy risk is crucial, affecting and being affected by other factors, indicating its pivotal role. Perceived fairness and usefulness are also influential, impacting service evaluations. Reputation dominates the peripheral path, reflecting users' emphasis on service quality and privacy risks based on past reputation.

In the motivation dimension (E13-E17), trust holds the highest centrality, aligning with Wang Yu chao's [4] finding that trust is essential for privacy sharing willingness. Users are more focused on whether their privacy will be protected, with service quality not being the foremost concern. Emotional value and reciprocity norm are also vital, as positive emotions and obligations encourage disclosure. In the capability dimension (E18-E19), privacy awareness's centrality and influence stand out. Heightened awareness affects risk and fairness assessments, as users scrutinize risks more with increased sensitivity, impacting judgments.

Causality Analysis.

There are a total of 9 causative factors and 10 outcome factors. Among these, user personality traits exhibit the highest causality (1.301), followed by material incentives (0.877), cognitive needs (0.837), and personalized services (0.711), indicating significant influences on other factors. User personality traits represent both users' urgency for services and their tolerance for privacy leaks. Hence, as a subjective decision-making behavior, privacy disclosure is significantly influenced by individual traits such as user personality and cognitive needs. Additionally, material incentives and personalized services also hold notable causality. These two factors essentially represent the value the service offers users, influencing perceived usefulness and subsequently affecting users' perception of utility and considerations of fairness.

In contrast, reciprocity norm (-1.072) and trust (-1.086) exhibit negative and relatively low causality values. Users' emotions, gratitude, and attachment to services are largely influenced by objective conditions such as service utility, further determining whether users trust the service or not.

5 Conclusions

Trust, cognitive needs, reputation, perceived privacy risk, perceived fairness, privacy awareness, user personality traits, and emotional value are among the crucial elements that the DEMATEL model extracts from the dimensions of the ELM model. This study highlights less-explored characteristics, including cognitive demands, user personality traits, emotional value, and reputation, while verifying criteria like trust and perceived privacy risk. Due to the subjective character of user qualities, they are frequently used as control variables. Even though it contributes to user happiness with individualized services, emotional value is frequently ignored. The motivation for privacy disclosure may increase emotional value for more individualized experiences. Within the online community, emotional value generates a sense of belonging and promotes information exchange. Reputation of a website, showing reliability, promotes trust, reduces privacy concerns, and encourages sharing.

Based on results, three suggestions are offered for enhancing privacy protection strategies. Firstly, service can analyze user personality traits and privacy sensitivity to ensure customer retention. Secondly, service should enhance user participation and interaction to cultivate emotional value. Thirdly, service should provide transparent disclosure of the source and destination of privacy data to improve perceived fairness.

References

1. China Internet Association. (2020) Analysis Report on Mobile Application Security Situation. https://www.isc.org.cn/article/40058.html
2. Zhang X, Chen X, Hou D. (2016) An Analysis of Online Health Information Disclosure Willingness Influencing Factors: An Integrated Model of TPB and Privacy Calculus. Information and Document Services, 01: 48-53. 10.3969/j.issn.1002-0314.2016.01.008
3. Wang Y.C., Sun Y.Q. (2018) The Influence of Service and Reciprocity Norms on Self-Disclosure Intention in Virtual Health Community[J]. Information Science, 36(05): 149-157. CNKI:SUN:QBKX.0.2018-05-026
4. Wang Y.C. (2018) Research on the Influencing Factors of Users' Health Information Disclosure Intention in Online Medical Community [J]. Journal of Information Resources Management, 8(01): 93-103. 10.13365/j.jirm.2018.01.093
5. Qiu J.P., Xu Z.Y., Chen X.H. (2023) Research on User Privacy Disclosure Behavior in Online Health Community Based on Tripartite Evolutionary Game[J]. Information Studies: Theo-ry&Practice,46(01):82-91.https://kns.cnki.net/kcms/detail/11.1762.G3.20220823.1148.006.html
6. Neys D W. (2012) Bias and Conflict: A Case for Logical Intuitions[J]. Perspectives on Psychological Science, 7(1): 28-38. 10.1177/1745691611429354
7. Dinev T, McConnell A R, Smith H J, et al. (2015) Information Privacy Research through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box[J]. Information Systems Research, 26(4): 639-655. http://dx.doi.org/10.1287/isre.2015.0600
8. Zhu G., Li F.J. (2022) Research on Mobile Health Privacy Disclosure Behavior under the Effect of Paradox Resolution[J]. Information studies: Theory &Application, 45(08):104-114. 10.16353/j/cnki.1000-7490.2022.08.015
9. Xu H, Dinev T, Smith J, et al. (2011) Information privacy concerns: Linking in-dividual perceptions with institutional privacy assurances[J]. Journal of the Association for Information Systems,12(12):798-824. 10.1108/10662241111104893
10. Culnan M.J., Pamela K.A. (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Sci-ence,10(1):104-115.10.1287/orsc.10.1.104
11. Wirtz J, Lwin M, Williams J D. (2007) Causes and consequences of consumer online privacy concern[J]. International Journal of Service Industry Management, 18(4):326-348. 10.1108/09564230710778128
12. Han P, Gu L, Zhang J.M. (2021) Research on Willingness to Share Medical Data from Perspective of Privacy Protection. Journal of Modern Information,41(03): 148-158.10.3969/j.issn.1008-0821.2021.03.015
13. Alhan A, Kaja J. F. (2021) Data privacy-related behavior and concerns of activity tracking technology users from Germany and the USA[J]. Journal of Information Management,73(2):180-200. 10.1108/AJIM-03-2020-0067
14. Dan J.K., Donald L. Ferrin, H.R.R. (2008) A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents[J]. Decision Support Systems,44(2):544-564. 10.1016/j.dss.2007.07.001

15. AHARONY N. (2016) Relationships among attachment theory, social capital per-spective, personality characteristics, and Facebook self-disclosure[J]. Journal of Infor-mation Management,68(3):362-386. info:doi/10.1108/AJIM-01-2016-0001
16. Nie Y.H., Luo J.Y. (2013) Perceived Usefulness, Trust and Personal Information Disclosure Intention of Social Networking Site Users. Documentation, Information &Knowledge (05):89-97. CNKI:SUN:TSQC.0.2013-05-011
17. Guo Y, Duan Q.S., Wang X.W. (2018) AN Empirical Study on Privacy Information Disclosure Behavior of Mobile Learning Users. Journal of Modern Infor-maiton,38(04):98-105. 10.3969/j.issn.1008-0821.2018.04.014
18. Zhu M.X, Wu C.H., Huang S.J., et al.(2021) Privacy Paradox in mHealth Applications: An Integrated Elaboration Likelihood Model Incorporating Privacy Calculus and Privacy Fatigue[J]. Telematics and Informatics, 61: 1-13. 10.1016/j.tele.2021.101601
19. Petty, Cacioppo J.(1986) The Elaboration Likelihood Model of Persuasion[J]. Advances in Experimental Social Psychology, 19: 123-205.