Asia Pacific Science Press

Asia Pacific Economic and Management Review
ISSN(O):3005-9275
ISSN(P):3005-9267
Vol. 1 No.2 (2024)

Exploring Configurational Factors Influencing Online Privacy Protection Behaviors of Internet Users

Huimin Liu, Ying Zhang*

Guangzhou College of Technology and Business, Guangzhou, 510000, China

Corresponding author: Ying Zhang, 18770770697@163.com

Abstract: With the rapid development of the digital economy, internet users' privacy protection behaviors have become a focal point for both academia and industry. This study adopts a configurational perspective and employs fuzzy-set Qualitative Comparative Analysis (fsQCA) to investigate the synergistic mechanisms of multiple factors influencing users' privacy protection behaviors. Integrating social cognitive theory, the research constructs an analytical framework encompassing individual cognitive factors (e.g., data privacy sensitivity, self-efficacy, perceived risks/benefits) and social-environmental factors (e.g., descriptive norms, subjective norms, platform trust). Based on 357 valid questionnaires, the study identifies core condition configurations driving high-level privacy protection behaviors. Key findings include: Five distinct paths explain high-level privacy protection behaviors, with "risk-benefit trade-off" (high perceived risk + low perceived benefit) and "social norm-driven" (high descriptive norms + high subjective norms) as typical patterns; Substitution effects exist between individual cognitive factors (e.g., self-efficacy) and environmental factors (e.g., platform trust), with different user groups relying on distinct condition combinations; Configurational analysis reveals "multiple conjunctural causality" in privacy behaviors, suggesting traditional linear regression may underestimate synergistic effects among variables. The study provides differentiated strategy insights for platforms to optimize privacy design and extends the application of privacy calculus theory in configurational analysis.

Keywords: Configuration Effects; Privacy Protection; Influencing Factors; Information Management

Published: Apr 15, 2024

DOI: https://doi.org/10.62177/apemr.v1i2.269

1.Introduction

In recent years, the proliferation of online social and economic activities has generated vast amounts of data. Enterprises frequently leverage collected information to enhance services for consumers. For instance, Didi utilizes passenger and driver location data to shorten waiting times and improve safety; Facebook employs personal data to curate posts and deliver targeted advertisements based on user preferences; online dating platforms analyze user information to recommend ideal matches. However, the ubiquitous availability of data has also led to adverse consequences. From Cambridge Analytica's exploitation of Facebook data to influence election outcomes, to health insurers predicting potential policyholders' health risks using undisclosed personal information, and private hackers targeting innocent users, privacy has emerged as one of the most critical challenges facing the digital economy.

The rapid development of mobile internet, characterized by its openness, innovation, information-sharing capabilities,

interactivity, and low cost, has fundamentally transformed how people access and share information. The rise of diverse social networking platforms and mobile devices has attracted massive user engagement, particularly in an era where 4G networks are widely accessible and 5G high-speed connectivity is rapidly penetrating all aspects of daily life, transforming societal development. Through self-presentation on social networks, individuals build interpersonal relationships and accumulate social capital. Yet, the openness of these platforms, while offering convenience, poses significant threats to user privacy. Consequently, investigating privacy protection behaviors in social networks holds significant theoretical and practical importance.

2.Literature Review

Regardless of the method employed to deliver targeted advertising, businesses must utilize users' personal information. The collection, sharing, sale, and use of such data inevitably heighten consumers' privacy concerns, which not only suppress individuals' willingness to disclose private information but also undermine the effectiveness of targeted ads. Evans(2009) analysis the evolution of internet advertising reveals that while targeted advertising represents an inevitable trend in the industry, it faces a fundamental and critical challenge: user privacy protection. Brandon(2013) argues that targeted ads enable consumers to better understand products, yet their reliance on personal data amplifies the risk of privacy breaches. Furthermore, the prevalent trading of consumer data in the market exacerbates user anxieties about information leakage. Zarouali (2017) through empirical analysis of retargeted ads on Facebook, demonstrate that when users exhibit low privacy concerns, targeted ads enhance purchase intentions, whereas this effect diminishes under heightened privacy concerns.

User privacy concerns directly impact corporate profitability, making effective privacy management a delicate yet essential task for businesses. From a firm-level perspective, Johnson's(2013) game-theoretic model shows that even when users employ ad-blocking tools, monopolistic firms can still profit. Vincent et al. find that when consumers can opt to block access to their purchase history, low blocking costs lead to widespread adoption, yet monopolistic enterprises remain profitable. Wang et al.,(2020) investigated the mechanisms through which privacy violation experiences influence self-disclosure behaviors, constructing a theoretical model through systematic stratified random sampling while integrating social contract theory and agency theory. Peng et al.,(2018) based on empirical research methodology and the trade-off between perceived risks and perceived benefits, concluded that privacy concerns jointly affect both privacy protection and information sharing behaviors. Cui et al.,(2019) employed game theory to enhance the practical utility of data in personalized differential privacy frameworks. Meanwhile, Sun et al.,(2020) modeled the conflicting incentives between service quality and privacy protection as an evolutionary game-theoretic model, effectively enabling users to Trade-off long-term service quality benefits against immediate privacy costs.

3.Research Design

3.1 Fuzzy-Set Qualitative Comparative Analysis (fsQCA)

This study employs Fuzzy-Set Qualitative Comparative Analysis (fsQCA) to investigate the causal relationships and mechanisms between conditional variables and outcome variables. fsQCA treats cases as configurations of conditions and outcomes, analyzing sufficiency and necessity relationships between conditional variables and outcomes to explore how these variables interact and jointly influence the results. The two most commonly used QCA approaches are crisp-set QCA (csQCA) and fuzzy-set QCA (fsQCA). While csQCA calibrates data into binary values (0 or 1), its dichotomous categorization risks oversimplification and information loss during data transformation. In contrast, fsQCA assigns continuous fuzzy membership scores ranging from 0 to 1, making it particularly suitable for handling continuous survey data. Since the numerical data obtained through the questionnaire survey in this study are continuous, fsQCA is a more appropriate methodological choice.

3.2 Selection of Research Variables

This study constructs an APCO model framework based on social cognitive theory to analyze antecedents and outcomes of privacy protection behaviors, selecting variables across two dimensions: individual cognition and social environment.

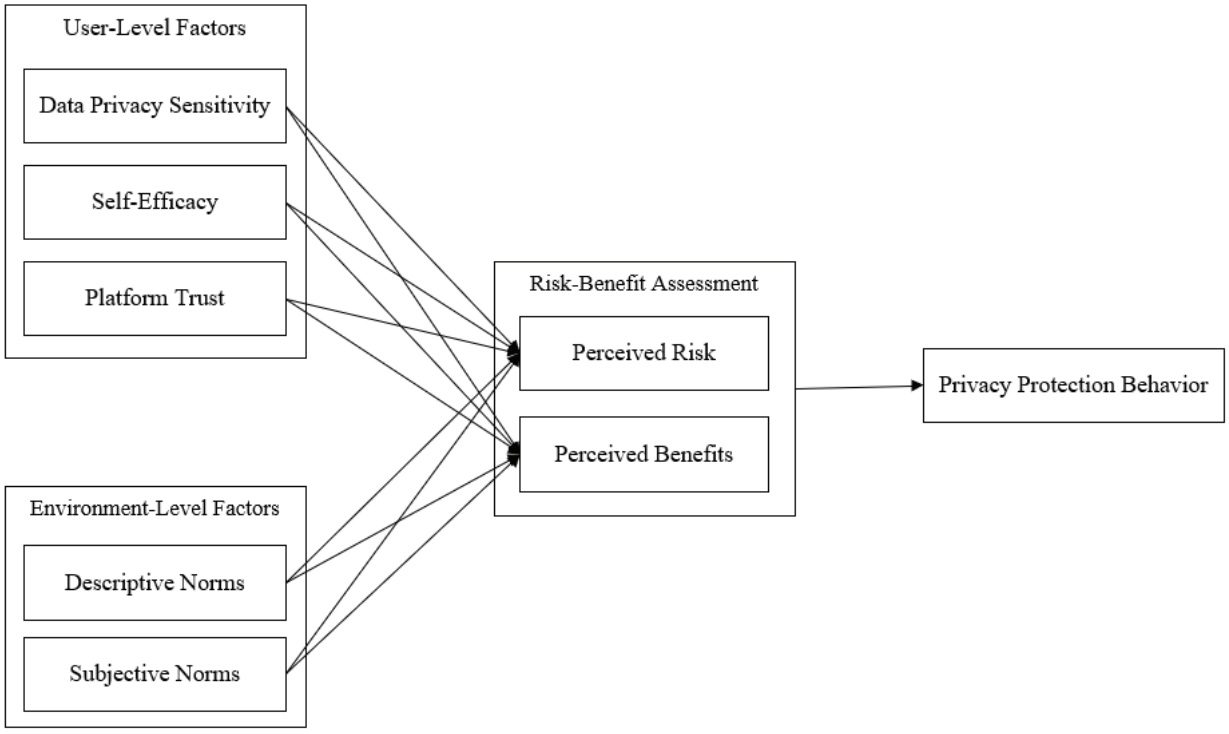
To clarify individuals' specific cognitive responses to security issues such as privacy breaches, this dimension is divided into three stages: ① Perception of Threat: Refers to the extent to which users perceive mobile IT security threats when

encountering privacy risks. ② Self-Efficacy and Response Efficacy:Self-efficacy denotes an individual's confidence in their ability to perform protective behaviors, which is tied to their perceived competence and access to resources.Response efficacy captures an individual's belief in the effectiveness of a protective behavior in mitigating threats. This evaluation is a cognitive process, forming judgments about the utility of such behaviors in addressing risks. ③ Perceived Privacy Value: Reflects a rational assessment of privacy's utility, where users weigh perceived costs (e.g., effort, inconvenience) against anticipated benefits (e.g., security, autonomy). According to social cognitive theory, individual cognition can exert measurable influence on the social environment.

Guided by social cognitive theory, two conditional variables are selected.Descriptive Norms: Describe the indirect social influence arising from widespread adoption of specific protective behaviors within a community. When individuals observe that a behavior is commonly practiced, they are more likely to adopt it themselves.Then, subjective Norms: Represent the perceived social pressure from significant others (e.g., family, friends) to engage in specific protective behaviors. Individuals often conform to these expectations to align with social approval. Empirical studies confirm that both descriptive and subjective norms significantly shape behavioral intentions.

The integrated conceptual model is illustrated in Figure 1.

Figure 1 Research Model



3.3 Data Collection: Questionnaire and Scale Design

This study employs a questionnaire and scale to collect user data. The questionnaire comprises three sections: an introduction, demographic characteristics survey, and measurement scales. A 5-point Likert scale is adopted to operationalize variables into multiple measurement items, with responses ranging from A (strongly disagree) to E (strongly agree). To ensure content validity, the scales were adapted from validated instruments used in prominent domestic and international studies, with linguistic adjustments tailored to this research context.

Prior to formal data collection, a pilot survey involving 20 participants was conducted from December 1 to 5, 2023, to refine the questionnaire structure, item sequencing, and wording of measurement items. Subsequently, considering that fuzzy-set Qualitative Comparative Analysis (fsQCA) prioritizes sample quality and representativeness over large sample sizes, a hybrid approach combining offline paper-based questionnaires and online electronic surveys was implemented from December 6 to 30, 2023. A total of 405 responses were collected. To address data quality concerns in online surveys, questionnaires with total completion times below 180 seconds (with a minimum response time of five seconds per question) were discarded,

resulting in 357 valid questionnaires.

3.4 Reliability and Validity Analysis of Scales

Reliability analysis serves as a critical method to evaluate the authenticity and accuracy of questionnaire data. This approach focuses on assessing the internal consistency and reliability of the data, typically measured using Cronbach's α coefficient. According to established standards (Hair et al., 2009; Huang et al., 2018), a Cronbach's α coefficient above 0.7 indicates acceptable internal consistency and reliable questionnaire quality, while values below 0.6 suggest significant discrepancies among scale items, rendering the data unsuitable for subsequent hypothesis testing.

In this study, reliability analysis revealed that all eight variables—privacy protection behaviors, data privacy sensitivity, self-efficacy, platform trust, descriptive norms, subjective norms, perceived risks, and perceived benefits—achieved Cronbach's α coefficients exceeding 0.7. These results confirm high internal consistency among the scale items and validate the questionnaires reliability. The scales used in this empirical study, along with their reliability test results, are summarized in Table 1.

Table 1 Reliability Test Results of the Questionnaire

Construct	Cronbach's α	Number
Privacy Protection Behavior (PP)	0.908	4
Data Privacy Sensitivity(DS)	0,918	3
Self-Efficacy(SE)	0.901	3
Platform Trust(ET)	0.889	3
Descriptive Norms(DN)	0.897	3
Subjective Norms(SN)	0.897	3
Perceived Risk(PR)	0.868	3
Perceived Benefits(PB)	0.769	3

Discriminant validity is used to determine whether measurement items genuinely reflect distinct variables or constructs, ensuring they are differentiated. Specifically, it verifies whether items should be assigned to separate factors or variables, thereby avoiding the measurement of divergent concepts under the same factor. As shown in Tables 2, the square roots of the average variance extracted (AVE) for all variables exceed the absolute values of their corresponding correlation coefficients. This indicates that while the variables exhibit moderate correlations, they remain statistically distinct. Consequently, the scales demonstrate satisfactory discriminant validity.

Table 2 Correlation Coefficient Matrix and Square Roots of AVE Test Results

	PP	DS	SE	ET	DN	SN	PR	PB
PP	0.797							
DS	0.262	0.811						
SE	0.402	0.365	0.781					
ET	-0.252	-0.071	-0.052	0.773				
DN	0.421	0.442	0.630	-0.131	0.807			
SN	0.342	0.526	0.501	-0.108	-0.180	0.785		
PR	0.379	-0.028	-0.377	0.678	0.619	-0.097	0.904	
PB	-0.361	0.372	0.323	0.687	0.591	-0.111	0.262	0.738

4.Data Analysis

4.1 Variable Calibration

Qualitative Comparative Analysis (QCA) operates on Boolean algebra principles, calibrating variables against specific sets to determine their degree of membership within those sets. The calibrated values obtained through this process serve as the foundation for subsequent data analysis.The calibration process transforms variables into sets by defining three critical thresholds:Full membership,Crossover point and Full non-membership.This study employs the direct calibration method to convert relevant antecedent and outcome variables into fuzzy-set membership scores, with transformed membership degrees ranging between 0 and 1.Following this methodology, the calibration anchor points for all variables are presented in Table 3.

Table 3 Calibration Anchor Points for Variables

Research Variables			Target Set	Anchor Points		
				Full Non-membership	Crossover Point	Full Membership
Conditional Variable	User-Level Factors	DS	High data privacy sensitivity	1	3	5
		SE	High self-efficacy	1	3	5
		ET	High platform trust	1	3	5
	Environment-Level Factors	DN	High descriptive norms	1	3	5
		SN	High subjective norms	1	3	5
		PR	High perceived risk	1	3	5
		PB	High perceived benefits	1	3	5
Outcome Variable		PP	high privacy protection behavior	1	3	5
			No-high privacy protection behavior	1	3	5

4.2 Necessary Condition Analysis

Prior to examining configurational effects, we first conducted a necessity analysis to determine whether individual antecedent conditions constitute necessary conditions for achieving specific outcomes (privacy protection/non-protection behaviors). Subsequently, for conditions that failed to demonstrate necessity individually, we performed sufficiency analysis to identify the most explanatory configuration of conditions for the outcome variables.The results of the necessary condition analysis are presented in Table 4.

Table 4 Necessary Condition Analysis

conditional variables	high privacy protection behavior	
	Consistency	Raw Coverage
High data privacy sensitivity	0.924	0.952
Low data privacy sensitivity	0.222	0.597
High self-efficacy	0.928	0.957

conditional variables	high privacy protection behavior	
	Consistency	Raw Coverage
Low self-efficacy	0.228	0.612
High platform trust	0.270	0.643
Low platform trust	0.879	0.953
High descriptive norms	0.949	0.955
Low descriptive norm	0.204	0.585
High subjective norms	0.948	0.951
Low subjective norms	0.201	0.582
High perceived risk	0.956	0.958
Low perceived risk	0.194	0.562
High perceived benefits	0.193	0.557
Low perceived benefits	0.947	0.951

As shown in Table 4, among the seven conditional variables influencing users' privacy protection behaviors, six variables demonstrate consistency scores exceeding 0.9: high data privacy sensitivity, high self-efficacy, high descriptive norms, high subjective norms, high perceived risks, and low perceived benefits. This indicates that these six variables constitute necessary conditions for privacy protection behaviors. These variables directly influence the outcome variable, meaning that without these six factors, users are unlikely to adopt any privacy protection measures. Meanwhile, low platform trust shows a consistency score above 0.8 but below 0.9, suggesting that while this variable exerts some influence on users' privacy protection behaviors, it does not qualify as a necessary condition.

4.3 Configurational Analysis

This study employed fsQCA 3.0 software for data analysis with a frequency threshold set at 1. Under the conditions of consistency scores exceeding 0.8 and PRI consistency greater than 0.75, we obtained the results presented in Table 5.The analysis revealed five distinct configurational paths influencing users' privacy protection behaviors, with consistency scores of 0.992, 0.992, 0.991, 0.972, and 0.992 respectively, indicating a high level of consistency. The overall solution consistency reached 0.986, demonstrating that 98.6% of individuals exhibited strong privacy protection behaviors under these five configurations, showing a clear and significant pattern. These results confirm the substantial impact of these configurations on privacy protection behaviors.Additionally, the overall solution coverage of 0.909 suggests that these five configurations can explain the privacy protection behaviors of 90.9% of the participants, indicating their strong explanatory power for high-level privacy protection behaviors. This finding further confirms that these configurations are prevalent within the sample and can be widely applied to improve and manage privacy protection behaviors.

Table 5 Configurational Paths of Conditional Variables

conditional variables	high privacy protection behavior				
	Path 1	Path 2	Path 3	Path 4	Path 5
Data Privacy Sensitivity (DS)				•	•
Self-Efficacy (SE)	•		•	•	•
Platform Trust (ET)	⊗	⊗			•
Descriptive Norms (DN)	•	•	•	•	•
Subjective Norms (SN)		•	•	⊗	

conditional variables	high privacy protection behavior				
	Path 1	Path 2	Path 3	Path 4	Path 5
Perceived Risk (PR)	•	•	•	•	•
Perceived Benefits (PB)	⊗	⊗	⊗	•	•
Consistency	0.992	0.992	0.991	0.976	0.992
Raw Coverage	0.813	0.825	0.873	0.138	0.142
Unique Coverage	0.007	0.020	0.066	0.001	0.003
Solution Consistency	0.986				
Solution Coverage	0.909				

Note：• indicates the presence of a core causal condition，⊗ indicates the absence of a core causal condition，• indicates the presence of a peripheral causal condition，Blank space indicates the condition may be either present or absent in the configuration.

5.Research Findings

The seven variables—data privacy sensitivity, self-efficacy, platform trust, descriptive norms, subjective norms, perceived risk, and perceived benefits—can be combined in five distinct configurations to explain high-level user privacy protection behaviors.

Path 1: SE*DN*PR*~PB*~ET.High self-efficacy+High descriptive norms+High perceived risk+Low perceived benefits+Low platform trust→High privacy protection behavior (raw coverage=0.813, consistency=0.992).For users with high self-efficacy, when they perceive that most people around them are cautious about cross-platform targeted recommendationsand refrain from easily providing personal information, their trust in platforms decreases. This elevates perceived risks and leads to strong privacy protection behaviors. Users confident in their ability to control personal information are significantly influenced by societal attitudes.

Path 2: DN*SN*PR~PB*~ET.High descriptive norms + High subjective norms+High perceived risk+Low perceived benefits+Low platform trust→High privacy protection behavior (raw coverage=0.825, consistency=0.992).This path highlights the combined influence of societal factors, perceived risk, perceived benefits, and platform trust. When both societal trends (e.g., general public caution) and close social circles (e.g., family/friends) express skepticism toward cross-platform targeted recommendations, users perceive greater privacy risks. As most users are risk-averse, they adopt a wait-and-see approach toward novel advertising models like cross-platform targeting. The collective societal stance amplifies privacy concerns, driving protective actions.

Paths 1 and 2 represent risk-benefit trade-off configurations, aligning with privacy calculus theory. When perceived risks outweigh benefits (high risk + low benefit), users rationally opt for privacy protection. Both paths cover >80% of the sample, indicating broad applicability.

Path 3: DS*SE*DN~SN*PR*PB.High self-efficacy + High descriptive norms + Low subjective norms + High perceived risk + High perceived benefits → High privacy protection behavior (raw coverage=0.873, consistency=0.991).Here, users confident in their ability to implement protective measures (high self-efficacy) and observing widespread privacy-conscious behaviors (high descriptive norms) still exhibit strong protection behaviors, despite the convenience and utility of cross-platform recommendations. High self-efficacy users feel their data is excessively controlled by third parties, heightening privacy concerns. Even when benefits are significant, perceived risks trigger protective actions.

Path 4: DS*SE*DN~SNPR*PB.High data privacy sensitivity+High self-efficacy+ High descriptive norms+Low subjective norms+High perceived risk+High perceived benefits→High privacy protection behavior (raw coverage=0.138, consistency=0.976).

This path emphasizes the interplay of individual traits and societal norms. Privacy-sensitive users actively monitor platform-

related risks and adopt protective measures, even when societal pressureis low.

Path 5: DS*SE*DN*PR*ET.High data privacy sensitivity + High self-efficacy + High descriptive norms + High perceived risk + High platform trust → High privacy protection behavior (raw coverage=0.142, consistency=0.992).Even users who trust platforms due to strong brand reputation or privacy policies may adopt protection behaviors if they are inherently privacy-sensitive and perceive high risks.

Paths 4 and 5 underscore that individual characteristics are pivotal in driving privacy behaviors, regardless of external incentives or trust.

Funding

1.Research on Human Resource Enhancement Strategies for Business Administration Majors Under the “Mass Entrepreneurship and Innovation” Initiative, 2024110144239.

2.Enhancement of Manufacturing Execution Efficiency and Service Performance Upgrade, KYHX2025062.

Conflict of Interests

The author(s)declare(s) that there is no conflict of interest regarding the publication of this paper.

References

[1] Evans DS. The online advertising industry: Economics, evolution, and privacy. Journal of Economic Perspectives, 2009,23(3)：37-60.

[2] Brandon SC. What’s mine is yours: Targeting privacy issues and determining the best solutions for behavioral advertising. The John Marshall Journal of Computer & Information Law, 2013, 29(4): 637-672.

[3] Zarouali B, Ponnet K. “Do you like cookies?” Adolescents’ skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. Computers in Human Behavior, 2017, (69): 157-165.

[4] Johnson JP. Targeted advertising and advertising avoidance. The RAND Journal of Economics，2013, 44(1): 128-144.

[5] Vincent C, Tay1or CR，Wagman L. Hide and seek: Costly consumer privacy in a market with repeat purchases. Marketing Science, 2012, 31(2) : 277-292.

[6] Wang Le, Wang Luyao Sun Zhao. The mechanism ofprivacy invasion experience on internet users’ self-disclo-sure[J]. System Engineering—Theory & Practice, 2020,40(1) : 79-92.

[7] Peng Lihui, Li He, Zhang Yanfeng, et al. Research on theinfluence factors of user privacy security on mobile socialmedia fatigue behavior —Based on privacy computingtheory of CAC research paradigm[J]. Information Science,2018, 36(9) : 96-102.

[8] Cui Lei, Qu Youyang, Nosouhi M R, et al. Improving datautility through game theory in personalized differential privacy [J] . Journal of Computer Science and Tech-nology, 2019, 34(2) : 272-286.

[9] Sun Zhe, Yin Lihua, Li Chao, et al. The QoS and Privacy Trade-off of adversarial deep learning: An evolutionary game approach[J] . Computers & Security, 2020, (96) :101876.