

**ANTECEDENTS OF PRIVACY CALCULUS AND
THE RELATIONSHIP WITH SOCIAL MEDIA
SELF-DISCLOSURE: THE MODERATING
ROLE OF ONLINE PRIVACY LITERACY**

ZHU LUHUI

UNIVERSITI SAINS MALAYSIA

2025

**ANTECEDENTS OF PRIVACY CALCULUS AND
THE RELATIONSHIP WITH SOCIAL MEDIA
SELF-DISCLOSURE: THE MODERATING
ROLE OF ONLINE PRIVACY LITERACY**

by

ZHU LUHUI

**Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy**

September 2025

ACKNOWLEDGEMENT

With profound gratitude and a heart full of warmth, I extend my deepest appreciation to those who illuminated my doctoral journey with unwavering support and kindness.

To my esteemed supervisor, Associate Professor Dr. Bahiyah Binti Omar, I owe an immeasurable debt of gratitude. Her wisdom, patience, and steadfast belief in my potential guided me through moments of doubt and inspired me to persevere. Her mentorship has been both a compass and an anchor, shaping not only this work but also my growth as a scholar. I am forever indebted to her for her patience, encouragement, and belief in my potential.

I am deeply thankful to Associate Professor Dr. Shuhaida Binti Md Noor, Dr. Nur Atikah Binti A Rahman and Dr. Rehan Tariq for their invaluable insights during the formative stages of this research. I am also profoundly thankful to Associate Professor Dr. Nor Ba'yah Abdul Kadir, Associate Professor Dr. Shuhaida Binti Md Noor, Professor Dr. Intan Hashimah Binti Mohd Hashim and the thesis examination committee for their time, the constructive feedback, and thoughtful suggestions to improve this study. My heartfelt thanks also go to all academic staff and non-academic staff of the School of Communication and Institute of Postgraduate Studies, USM. I extend my appreciation to all the necessary help and continued support they provided.

To my beloved parents, my siblings, and my dearest spouse, their selfless support and unwavering encouragement gave me the peace of mind to pursue this academic journey wholeheartedly.

May the light they have kindled within me continue to shine forward.

TABLE OF CONTENTS

ACKNOWLEDGEMENT.....	ii
TABLE OF CONTENTS.....	iii
LIST OF TABLES.....	ix
LIST OF FIGURES	xi
LIST OF ABBREVIATIONS	xii
LIST OF APPENDICES.....	xiii
ABSTRAK	xiv
ABSTRACT	xvi
CHAPTER 1 INTRODUCTION	1
1.1 Introduction.....	1
1.2 Background of the Study.....	1
1.2.1 Study Background in China	6
1.3 Problem Statement	9
1.4 Research Objectives	19
1.5 Research Questions	20
1.6 Scope of the Study	21
1.7 Significance of the Study	22
1.7.1 Theoretical Significance	22
1.7.2 Methodological Significance	24
1.7.3 Practical Significance.....	25
1.8 Conceptualization of the Variables	27
1.8.1 Social Media Self-Disclosure (SMSD)	27
1.8.2 Perceived Benefits (PB).....	28
1.8.2(a) Perceived Security (PSEC)	29
1.8.2(b) Personalized Service (PSER).....	29

1.8.2(c)	Social Connection (SC)	30
1.8.3	Perceived Risks (PR)	30
1.8.3(a)	Privacy Concerns (PC).....	31
1.8.3(b)	Perceived Intrusion (PI)	31
1.8.3(c)	Perceived Severity (PSEV).....	31
1.8.4	Individual Privacy Perception (IPP)	32
1.8.4(a)	Privacy Awareness (PA).....	32
1.8.4(b)	Information Sensitivity (IS)	32
1.8.5	Platform Privacy Assurance (PPA)	33
1.8.5(a)	Effectiveness of Privacy Policy (EPP).....	33
1.8.5(b)	Privacy Settings (PSET)	34
1.8.6	Information Asymmetry (IA)	34
1.8.7	Government Regulation (GR).....	35
1.8.8	Online Privacy Literacy (OPL)	36
1.9	Overview of the Thesis	36
CHAPTER 2 LITERATURE REVIEW		38
2.1	Introduction	38
2.2	Self-Disclosure: Evolution and Social Role.....	38
2.2.1	Evolution of Digital Self-Disclosure.....	38
2.2.2	Social Role: Double-Edged Sword	42
2.3	Information Privacy in China.....	46
2.4	Digital Privacy Invasion and Strategies to Overcome It.....	51
2.5	Past Studies on Self-Disclosure and Privacy	55
2.6	Theoretical Lens: Privacy Calculus Theory	64
2.6.1	Justification for Privacy Calculus Theory	65
2.6.1(a)	Technology Acceptance Model.....	65
2.6.1(b)	Communication Privacy Management Theory	67

2.6.1(c)	Social Exchange Theory	68
2.6.1(d)	Self-Presentation Theory	68
2.6.1(e)	Uses and Gratifications Theory	70
2.6.2	Overview of Privacy Calculus Theory	71
2.6.3	Perceived Benefits and Perceived Risks	73
2.7	Research Model and Development of Hypotheses	76
2.7.1	Privacy Calculus and Social Media Self-Disclosure.....	77
2.7.1(a)	Perceived Benefits and Social Media Self-Disclosure	77
2.7.1(b)	Perceived Risks and Social Media Self-Disclosure	80
2.7.2	Antecedents and Consequences of Privacy Calculus on Social Media Self-Disclosure.....	82
2.7.2(a)	Individual Privacy Perception (Privacy Awareness, Information Sensitivity)	82
2.7.2(b)	Platform Privacy Assurance (Effectiveness of Privacy Policy, Privacy Settings).....	86
2.7.2(c)	Information Asymmetry	89
2.7.2(d)	Government Regulation	91
2.7.3	Perceived Benefits and Perceived Risks as Mediating Factors.....	93
2.7.4	Online Privacy Literacy as Moderating Factor	96
2.7.5	Control Variables.....	99
2.8	Research Model.....	101
2.9	Hypotheses Statement	104
2.10	Summary of the Chapter	106
CHAPTER 3 METHODOLOGY		108
3.1	Introduction.....	108
3.2	Research Paradigm.....	108
3.3	Research Design.....	110
3.4	The Survey Method.....	113

3.5	Population and Sampling of the Study.....	116
3.5.1	Target Population: Inclusion and Exclusion Criteria	116
3.5.2	Sample Size.....	119
3.6	Sampling Techniques	122
3.6.1	Purposive Sampling Technique.....	123
3.6.2	Snowball Sampling Technique.....	125
3.7	Operationalization and Measurement of the Variables	127
3.7.1	Individual Privacy Perception (IPP)	128
3.7.2	Platform Privacy Assurance (PPA)	129
3.7.3	Information Asymmetry (IA).....	131
3.7.4	Government Regulation (GR).....	131
3.7.5	Perceived Benefits (PB).....	132
3.7.6	Perceived Risks (PR)	134
3.7.7	Social Media Self-Disclosure (SMSD).....	136
3.7.8	Online Privacy Literacy (OPL).....	137
3.8	The Research Instrument	138
3.8.1	Questionnaire Design.....	138
3.9	Expert Review.....	141
3.10	Ethical Review and Consent	143
3.11	Pilot Test.....	143
3.12	Data Collection	146
3.13	Statistical Analyses	148
3.13.1	Descriptive analysis	148
3.13.2	Partial Least Square Structural Equation Modeling (PLS-SEM).....	148
3.13.3	Measurement Model Assessment.....	152
3.13.3(a)	Assessment of Reflective Constructs.....	152
3.13.3(b)	Assessment of Formative Constructs.....	155

3.13.4	Mediation Effect Assessment.....	160
3.13.5	Moderation Effect Assessment.....	162
3.14	Preliminary Data Analysis	163
3.14.1	Normality Test.....	163
3.14.1(a)	The Shapiro-Wilk Test	164
3.14.1(b)	The Kolmogorov-Smirnov test	165
3.14.1(c)	Mardia's Multivariate Skewness and Kurtosis of Normality Test	166
3.14.2	Common Method Variance (CMV).....	167
3.14.2(a)	Harman's Single-Factor Test.....	168
3.14.2(b)	Marker Variable Technique	172
3.15	Summary of the Chapter	174
CHAPTER 4 DATA ANALYSIS		176
4.1	Introduction.....	176
4.2	Preparation of Data Analysis.....	176
4.2.1	Data Cleansing	176
4.3	Descriptive Analysis	177
4.3.1	Demographic Analysis Frequency of Respondents' Profiles	177
4.3.2	Descriptive Analysis of Variables and Instrument	180
4.4	Measurement Model	181
4.4.1	Internal Consistency Reliability	182
4.4.2	Indicator Reliability (Outer Loadings).....	185
4.4.3	Convergent Validity	185
4.4.4	Discriminant Validity	186
4.4.5	Estimating the Formative Higher-Order Constructs	193
4.5	Structural Model	195
4.5.1	Structural Model for Collinearity Issues Assessment	195
4.5.2	Significance of the Structural Model Relationships Assessment.....	196

4.5.2(a)	Hypothesis Testing for Direct Effects	196
4.5.2(b)	Hypothesis Testing for Mediation Effects	200
4.5.2(c)	Hypothesis Testing for Moderation Effects	205
4.5.3	Coefficient of Determination (R ²) and Predictive Relevance (Q ²)	206
4.5.4	Effect Size Assessment (f^2)	207
4.5.5	Important-Performance Map Analysis (IPMA)	208
4.5.6	PLS Predictive Analysis	211
4.6	Summary of the Chapter	216
CHAPTER 5 DISCUSSION AND CONCLUSION		218
5.1	Introduction	218
5.2	Summary of the Findings	218
5.3	Discussion of the Findings	222
5.4	Research Implications	240
5.4.1	Perceived Benefits vs. Perceived Risks on Social Media Self-Disclosure	241
5.4.2	The role of Platform vs. Government in Promoting Social Media Self-Disclosure	242
5.4.3	The Negative Influence of Individual Privacy Perception and Information Asymmetry	243
5.4.4	The Role and Implications of Online Privacy Literacy	244
5.5	Contributions of the Study	246
5.5.1	Theoretical Contribution	246
5.5.2	Methodological Contribution	249
5.5.3	Practical Contribution	253
5.6	Limitations and Recommendations for Future Research	258
5.7	Conclusion	260
REFERENCES		262
APPENDICES		

LIST OF TABLES

	Page
Table 1.1 The Gap in Prior Studies on Social Media Self-Disclosure.....	18
Table 2.1 Parts of Chinese Personal Information Laws.....	49
Table 2.2 Prior studies on Self-Disclosure and Privacy.....	60
Table 3.1 The Structure of Chinese Social Media Users	116
Table 3.2 Penetration Rate of Major Social Media in China and Henan Province	118
Table 3.3 Inclusion Criteria and Exclusion Criteria of Sample	119
Table 3.4 Distribution of Seeds (n=45).....	125
Table 3.5 Measurement Items for Individual Privacy Perception.....	128
Table 3.6 Measurement Items for Platform Privacy Assurance.....	130
Table 3.7 Measurement Items for Information Asymmetry.....	131
Table 3.8 Measurement Items for Government Regulation.....	132
Table 3.9 Measurement Items for Perceived Benefits	133
Table 3.10 Measurement Items for Perceived Risks.....	134
Table 3.11 Measurement Items for Social Media Self-Disclosure	136
Table 3.12 Measurement Items for Online Privacy Literacy	137
Table 3.13 Constructs of the Study	140
Table 3.14 Demographic Factors for Pilot Test (n=168)	144
Table 3.15 Cronbach's Alpha for Pilot Test	145
Table 3.16 Guidelines of Measurement Model Assessment	156
Table 3.17 Guidelines of Structural Model Assessment	159
Table 3.18 Results of Shapiro-Wilk Test	164
Table 3.19 Results of Kolmogorov-Smirnov Test	165
Table 3.20 Results of Mardia's Multivariate Skewness and Kurtosis Test.....	166
Table 3.21 Harman's Single Factor-Test.....	169

Table 3.22	Correlation between the Marker Variable and Main Variables	173
Table 3.23	Comparison of Path Coefficients between Baseline Model and Marker Model	173
Table 3.24	Comparison of R ² between Baseline Model and Marker Model	174
Table 4.1	Demographic Profile of Respondents (n=761)	178
Table 4.2	Descriptive Analysis of Variables	181
Table 4.3	Results Summary for Unidimensional Constructs	183
Table 4.4	Fornell-Larcker Criterion	187
Table 4.5	Cross Loading	188
Table 4.6	Heterotrait Monotrait (HTMT) Criterion	192
Table 4.7	Results Summary for Higher-Order Multidimensional Constructs.....	194
Table 4.8	Variance Inflation Factors (VIFs) Test.....	195
Table 4.9	Result Summary of the Direct Effect Tests	199
Table 4.10	Result Summary of the Mediation Effect Tests	204
Table 4.11	VAF of Mediation Effects	204
Table 4.12	Result Summary of the Moderation Effect Tests	206
Table 4.13	Summary of R ² value and Q ² value	207
Table 4.14	Summary of Effect Size: f^2	208
Table 4.15	Results of Important Performance of Social Media Self-Disclosure.....	209
Table 4.16	Results of PLS Predict	212
Table 4.17	CVPAT LV Summary for Model Comparison	214
Table 5.1	Summary of Research Objectives and Hypotheses Results.....	220

LIST OF FIGURES

	Page
Figure 2.1 The Conceptual Framework.....	103
Figure 3.1 Research design of the current study	112
Figure 3.2 Sample size rule of Green (1991)	122
Figure 4.1 The Important-Performance Map of SMSD	210
Figure 4.2 Model 1: Established Model (Validated Model)	215
Figure 4.3 Model 2: Alternative Model.....	215

LIST OF ABBREVIATIONS

EPP	Effectiveness of Privacy Policy
GR	Government Regulation
IA	Information Asymmetry
IPP	Individual Privacy Perception
IS	Information Sensitivity
OLP	Online Privacy Literacy
PA	Privacy Awareness
PB	Perceived Benefits
PC	Privacy Concerns
PI	Perceived Intrusion
PPA	Platform Privacy Assurance
PR	Perceived Risks
PSEC	Perceived Security
PSER	Personalized Service
PSET	Privacy Settings
PSEV	Perceived Severity
SC	Social Connection
SMSD	Social Media Self-Disclosure

LIST OF APPENDICES

Appendix A	Questionnaire (English Version)
Appendix B	Questionnaire (Chinese Version)

**ANTESEDEN KEPADA KALKULUS PRIVASI DAN HUBUNGANNYA
DENGAN PENDEDAHAN DIRI DI MEDIA SOSIAL: PERANAN
MODERASI CELIK PRIVASI DALAM TALIAN**

ABSTRAK

Dengan peningkatan pendedahan diri di media sosial, kebimbangan terhadap privasi dalam talian turut meningkat dengan ketara. Bagi memahami dengan lebih mendalam mekanisme di sebalik tingkah laku ini, kajian ini menggunakan Teori Kalkulus Privasi sebagai asas teori dan meneliti bagaimana faedah yang dirasakan (perceived benefits) dan risiko yang dirasakan (perceived risks) mempengaruhi pendedahan diri, bersama empat anteseden iaitu persepsi privasi individu, jaminan privasi platform, asimetri maklumat, dan peraturan kerajaan. Reka bentuk kuantitatif dengan Pemodelan Persamaan Struktural Partial Least Squares (PLS-SEM) telah digunakan untuk menganalisis data daripada 761 pengguna media sosial di China. Hasil kajian menunjukkan beberapa penemuan signifikan: faedah yang dirasakan mempunyai pengaruh positif yang kuat terhadap pendedahan diri, manakala risiko yang dirasakan menghalang pendedahan tersebut secara signifikan. Pada tahap anteseden, persepsi privasi individu secara signifikan meningkatkan risiko yang dirasakan; jaminan privasi platform secara signifikan meningkatkan faedah yang dirasakan dan mengurangkan risiko; asimetri maklumat secara signifikan mengurangkan faedah yang dirasakan; manakala peraturan kerajaan secara signifikan meningkatkan faedah yang dirasakan tetapi tidak memberi kesan signifikan terhadap risiko. Ujian mediasi selanjutnya menunjukkan bahawa faedah yang dirasakan secara signifikan memediasi pengaruh jaminan privasi platform, asimetri maklumat, dan peraturan kerajaan terhadap pendedahan diri, manakala risiko yang dirasakan memediasi kesan persepsi

privasi individu dan jaminan privasi platform. Literasi privasi dalam talian turut diuji sebagai moderator, namun kesannya terhadap hubungan faedah–risiko–pendedahan didapati tidak signifikan. Dari segi teori, kajian ini memperluas kalkulus privasi dengan memperkenalkan anteseden peringkat individu dan platform sebagai konstruk peringkat tinggi serta menggabungkan literasi privasi dalam talian, sekali gus memperkayakan penjelasan mengenai pengambilan keputusan berkaitan privasi. Dari segi metodologi, penggunaan konstruk reflektif–formatif dan teknik pembolehubah penanda mengukuhkan kekukuhan dapatan serta menangani bias kaedah bersama. Dari segi praktikal, kajian ini memberikan implikasi berharga kepada pembangun platform dan penggubal dasar dengan menekankan keperluan untuk memperkukuh ciri privasi platform, mengurangkan risiko penyalahgunaan maklumat, serta mempertingkatkan perlindungan peraturan bagi menjaga data pengguna. Secara keseluruhan, dapatan kajian ini mengesahkan pertukaran kritikal antara risiko dan faedah yang dirasakan dalam membentuk pendedahan diri di media sosial serta menyediakan cadangan berasaskan bukti bagi mewujudkan persekitaran dalam talian yang lebih selamat.

**ANTECEDENTS OF PRIVACY CALCULUS AND THE RELATIONSHIP
WITH SOCIAL MEDIA SELF-DISCLOSURE: THE MODERATING
ROLE OF ONLINE PRIVACY LITERACY**

ABSTRACT

With the increasing prevalence of social media self-disclosure, concerns over online privacy have grown significantly. To better understand the mechanisms underlying such behaviors, this study employs the Privacy Calculus Theory as its foundation and examines how perceived benefits and perceived risks influence disclosure, together with four antecedents: individual privacy perception, platform privacy assurance, information asymmetry, and government regulation. A quantitative design with Partial Least Squares Structural Equation Modeling (PLS-SEM) was used to analyze data from 761 Chinese social media users. The results reveal several significant findings: perceived benefits strongly and positively influence self-disclosure, while perceived risks significantly deter it. At the antecedent level, individual privacy perception significantly increases perceived risks; platform privacy assurance significantly enhances perceived benefits and reduces risks; information asymmetry significantly reduces perceived benefits; and government regulation significantly improves perceived benefits but shows no significant effect on risks. Mediation tests further demonstrate that perceived benefits significantly mediate the influence of platform privacy assurance, information asymmetry, and government regulation on disclosure, whereas perceived risks significantly mediate the effects of individual privacy perception and platform privacy assurance. Online privacy literacy was also tested as a moderator, but its effects on the benefit–risk–disclosure relationships were statistically insignificant. Theoretically, the study extends privacy

calculus by introducing both individual- and platform-level antecedents as higher-order constructs and incorporating online privacy literacy into the model, thereby enriching the explanation of privacy-related decision-making. Methodologically, the application of reflective–formative constructs and marker variable techniques strengthens the robustness of the findings and addresses common method bias. In practical terms, the study offers valuable implications for platform developers and policymakers by emphasizing the necessity of enhancing platform privacy features, reducing risks of information misuse, and strengthening regulatory safeguards to protect users’ data. Overall, the findings confirm the critical trade-off between perceived risks and benefits in shaping social media self-disclosure and provide evidence-based recommendations for creating safer online environments.

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter introduces the research topic of the study. First, the research background of self-disclosure is introduced. Self-disclosure is beneficial to both social media platforms and users, but it also triggers privacy issues. Then, the problems existing in the research related to privacy and self-disclosure are stated, and the research objectives and research questions of this study are proposed based on this. Subsequently, the scope of the study is determined, and then the significance is pointed out. Finally, the various variables involved in the study are conceptualized.

1.2 Background of the Study

As an essential form of communication, disclosing information about oneself is one of the most common behaviors for individuals in their daily lives. Approximately 30-40% of everyday conversation is utilized to convey information about private experiences and personal relationships (Tamir & Mitchell, 2012). With the rise of social media and the maturity of communication technology, disclosing information has changed from early word-of-mouth to the present disclosing online (Chung et al., 2021).

Due to its convenience and benefits, disclosing information on social media has become one of the most popular online activities nowadays (Apuke & Omar, 2021c). In the past few years, a few social media platforms have rapidly spread around the world. To date, it has become the main tool for people to communicate and disclose information about themselves on their hobbies, experiences, and day-to-day lives

(Jung, 2017). According to a recent statistic from Kemp (2024), as of January 2024, more than 5 billion people are actively using social media tools daily, accounting for 62.3% of the world's total population. In this study, social media self-disclosure is defined as the act of voluntarily revealing personal information, which may take different forms depending on the user's purpose and context. On one hand, it refers to the disclosure of factual or identifiable data, such as name, age, contact details, location, or demographic background, which can be used to establish one's digital identity. On the other hand, it also encompasses the sharing of subjective experiences and personal expressions, including daily life updates, photos, emotions, opinions, and interpersonal interactions. Such disclosures serve not only functional needs, such as accessing services or maintaining online accounts, but also social and psychological purposes, such as fostering social connections, obtaining support, and performing self-presentation.

Meanwhile, data and information are very crucial for the production of the social media business model (Lee et al., 2022; Naous et al., 2019). The fundamental success of any social media platforms largely depend on users' active disclosing and sharing behaviors (Z. Liu et al., 2022). Social media platforms can leverage tools like opinion mining and sentiment analysis to consistently collect vast amounts of user data, often with users' awareness and consent, and use this information to deliver personalized services, thereby attracting a larger user base and ensuring long-term business growth (Chen, 2018; Gandomi & Haider, 2015).

The rapid proliferation of social media as a means of information sharing offers significant commercial advantages for platforms and practical utility for users (Tuten, 2023). However, this increasing disclosure also raises substantial concerns regarding privacy invasions. Privacy invasion denotes situations in which individuals perceive a

violation of their privacy, resulting in negative emotions, such as anger and resentment (Lu & Yi, 2023; Pang & Ruan, 2023). It results from perceived violations of personal space by others (Hunecke et al., 2021). In this study, privacy invasion implies that social media users have been unwittingly exposed to search and seizure, creation of databases consisting of personal information, and improper usage of that information by a third party.

Information disclosed by users may be misused by some social media platforms without their knowledge. For instance, the famous “Cambridge Analytica scandal” is one of the most heavily published privacy invasion issues; around 87 million Facebook users’ privacy data were illicitly harvested without their consent, aiming to influence users’ voting decisions in the 2016 United States presidential election (Hinds et al., 2020). Improper use of private information by third parties may endanger property and even personal safety. The case of Chinese actor Wang Xing serves as a cautionary example (Dowling, 2025). In the beginning of 2025, Wang Xing was lured to Myanmar Scam Park via Thailand since his personal information, including details about contact information, career, and interests, had been gleaned from his public social media profiles by a fraudulent network. The perpetrators used this information to craft a convincing offer tailored to his aspirations, ultimately trapping him in an online fraud operation. Although Wang Xing was rescued jointly by the Thai and Chinese governments, similar cases are not uncommon. It is reported that about 70,000 Chinese people are defrauded every year through online platforms (Sheng, 2025). This incident highlights the negative consequences of sharing sensitive or excessive personal information on the internet.

Among various forms of online privacy breaches, social media has been identified as the leading source of personal data leaks. A survey conducted among

1,000 U.S. residents (Proton, 2022) revealed that 42.12% had experienced privacy violations on social media platforms, surpassing other digital environments such as online gaming (25%) and technology-focused websites (20.55%). Boston Consulting Group predicts that the number of users who perceive personal information misuse will dramatically increase in the next few years because of increased social media use (Baltassis et al., 2018). With cyberattacks, online stalking, and improper use of users' data occasionally occurring, it is unsurprising that such privacy invasion can't be totally avoidable for the foreseeable future.

The rising incidence of data breaches on social media platforms has heightened concerns surrounding privacy and information security. As a result, both scholars and industry practitioners are actively exploring ways to strike an effective balance between maximizing users' willingness to self-disclose and minimizing potential privacy risks to the greatest extent possible (Ma et al., 2021).

The motivation of this study arises from the urgent need to understand this tension. On one side, self-disclosure is indispensable for building online relationships, sustaining platform engagement, and enabling personalized services. On the other side, privacy invasion remains a serious threat with profound social, psychological, and even economic consequences. Without deeper empirical insights into the mechanisms shaping users' disclosure behavior, it is difficult to inform policy, guide platform governance, or design effective interventions to enhance both user safety and user experience. This dual significance makes social media self-disclosure a highly relevant and important research focus in both academic and practical domains.

Despite the fact that the risks of privacy invasion have increased in the context of social media, users continue to disclose their personal information for a variety of

benefits, such as social connection and platform services (Debatin et al., 2009). This inconsistency between users' self-disclosure actions and their worries regarding privacy threats has been labelled as the "privacy paradox" (Barnes, 2006; Kokolakis, 2017; Norberg et al., 2007). The privacy paradox highlights that users often weigh the perceived advantages and potential threats of sharing personal information when navigating social media environments (Dinev & Hart, 2006).

Researchers suggest that individuals engage in an internal privacy calculus when making privacy-related decisions, whereby their actions are guided by the outcome of a perceived trade-off between risks and benefits (Chen, 2018; Jozani et al., 2020; L. Wang et al., 2020). Privacy calculus refers to the subjective cost-benefit analysis individuals perform when prompted to share personal information in exchange for a product or service; self-disclosure occurs when the perceived benefits outweigh the potential risks of privacy loss (Jozani et al., 2020). The outcome behavior of an individual's privacy calculus is influenced by many antecedent factors (Kim et al., 2019). Privacy calculus is a rigorous model to study privacy-related information disclosure behavior in the context of social media (Hassandoust et al., 2020). The privacy calculus model shows that people decide whether to disclose their personal information based on the outcomes of a calculation from perceived benefits and perceived risks in a specific information-disclosing context (Xu et al., 2014).

In addition, as individuals become more familiar with social media and pay more attention to privacy issues, differences in online privacy literacy have emerged (Kaya & Yaman, 2022). Research suggests that online privacy literacy is a crucial factor influencing online behavior, particularly in the context of privacy-related decisions (Bartsch & Dienlin, 2016; Ma & Chen, 2023; Masur, 2020). However, how

online privacy literacy moderates individuals' privacy calculus and, in turn, affects social media self-disclosure remains an open question.

In summary, this study aims to explore the influencing factors of social media self-disclosure. Based on the privacy calculus theory, this study examines the influence of users' perceived benefits and perceived risks on self-disclosure in social media and studies the effects of antecedents. In addition, the moderating role of online privacy literacy in this relationship is also investigated in this study.

1.2.1 Study Background in China

China has one of the largest internet populations globally. According to a Chinese data report (CNNIC, 2024), as of June 2024, Chinese netizens reached 1.099 billion, with a 78% internet penetration rate, and 99.7% accessing the internet via mobile phones. China also has the world's most active social media environment, with 1.077 billion users (CNNIC, 2024), nearly equating to the total number of netizens. The rapid development of the social media industry is driven by innovations like Mini Programs and Channels, with WeChat's Mini Programs exceeding 450 million daily active users in 2022 (Tencent, 2022). Given the expanding user base and technological advancements, China provides a rich context for social media research.

In the early 2000s, some social media companies were short of complete user privacy protection strategies in China. Kong (2007) found that Chinese social media companies collected a vast amount of personal data on their websites and that only about half of them have privacy policies or statements. The emerging technology forces have not yet threatened the privacy and information security of individuals at that age (Millett et al., 2007). Therefore, privacy protection did not come to the

attention of the public. In the second decade of the new millennium, Chinese Internet regulation still lagged far behind the technology, leading to widespread privacy violations (Lee, 2014). Wu et al. (2011) conducted a study comparing internet privacy legislation in the United States and China, discovering that American legislative protections were more thorough and extensive than those of China; they noted that the principal method for protecting users' online privacy in China relies on platform self-regulation.

In recent years, the probability of users' personal information being exposed on the Internet has been rising, and such privacy invasions have largely threatened users' interests in China (Sun et al., 2017); Notable incidents include the 2017 Cainiao-SF Express dispute (Yu & He, 2021) and the 2018 Alipay "default check" controversy (Yu & He, 2021). A 2021 report found that 63.4% of netizens experienced leaks of browsing histories and IP addresses, while 78.2% reported exposure of personal details like phone numbers and emails (Hu, 2021). These situations show that privacy invasion is no longer an accidental incident but a public event that needs to attract people's attention.

In the field of social media, the 2020 Weibo "celebrity phone number leak" incident exposed not only the privacy of public figures but also raised concerns among ordinary users about the platform's privacy protection measures (Zhang, 2020). As a result, many users reduced the use of real phone numbers on Weibo or opted for anonymous registrations to protect their privacy. Additionally, controversies about the misuse of facial recognition technology on short video platforms heightened fears of personal privacy being "monitored by algorithms" (Lei, 2021). These incidents highlight the growing demand for privacy protections among social media users.

In June 2017, the Cybersecurity Act in China was published. This is the first time establishing the general meaning of “personal information” at the legal level in China (Liu et al., 2021). Subsequently, the first Chinese Data Security Act was published in 2018. Privacy legislation in China has been evolving in recent years. In November 2021, the Chinese government implemented the Personal Information Protection Act (PIPA) to protect people’s information security from privacy invasion by service providers or third parties due to misusing personal information (You, 2022). Since then, online personal information and digital data security have been guarded by government laws and regulations in China.

Despite legislative progress, Chinese academic research on social media privacy and self-disclosure remains limited. Most empirical studies are based in Western contexts (Lee et al., 2022). Chinese perceptions of privacy and self-disclosure practices in social media have not been fully examined (L. Wang et al., 2020). Since privacy concerns differ across nations (Chen & Tsoi, 2011; Lin et al., 2012), further research is needed to explore online privacy in China. In this way, online privacy protection can be enhanced, and self-disclosure can be encouraged in the context of Chinese social media settings.

Considering these factors, China provides an appropriate and significant context for this research. The country’s vast internet population, diverse and highly active social media platforms, and rapidly evolving technological landscape create both opportunities and challenges for privacy management and self-disclosure. At the same time, the prevalence of privacy invasion incidents, together with the relatively recent development of privacy legislation and ongoing public concerns, highlights the urgency of conducting an in-depth examination of social media privacy and disclosure behaviors in the Chinese context. Therefore, this study is situated in China, aiming to

generate insights that can contribute to both theoretical understanding and practical improvements in online privacy protection and self-disclosure practices.

1.3 Problem Statement

With the increasing reliance on social media for communication, information sharing, and other activities, social media platforms have evolved into critical nodes for accumulating information and data (Van der Schyff et al., 2020). Central to these interactions is users' self-disclosure behavior, which influences their social experiences and presents considerable privacy concerns. Understanding the factors influencing users' self-disclosure behavior is essential for social media providers to sustain platform growth and address users' privacy concerns (Cheung et al., 2015). Despite the growing body of social media self-disclosure research, gaps and unresolved issues remain in the literature (Beigi & Liu, 2020; Efe & Suliman, 2021).

Firstly, there is a mixed understanding of the effects of privacy concerns on social media self-disclosure (Cain & Imre, 2021). Specifically, one line of research argues that online privacy concerns have little to no influence on self-disclosure in SNS, whereas another stream contends that such concerns do affect users' disclosure behavior. For example, Reynolds et al. (2011) discovered a minimal link between participants' general concern regarding privacy on Facebook and their posting behaviors. Similarly, Hughes-Roberts (2013) concluded, based on an analysis of participants' Facebook profiles, that a general declaration regarding user privacy concerns is not a valid indicator of disclosure behavior. Barth et al. (2019) devised an experiment regarding the privacy paradox and discovered that privacy concerns did not significantly influence users' paradoxical behavior; specifically, individuals

declare themselves to be truly concerned about their privacy, yet their behaviors indicate that privacy is not their crucial priority.

On the other hand, Lut et al. (2018) have different opinions; they analyzed the relationship between disclosure and privacy by investigating the privacy risks linked to online self-disclosure, which showed privacy concerns influence the intensity of disclosure. Gruzd and Hernández-García (2018) recognized five dimensions of self-disclosure (i.e., amount, depth, polarity, accuracy, and intent) and discovered moderate associations between privacy concerns and several dimensions of self-disclosure (i.e., amount, depth, and accuracy). This indicated that varying privacy concerns may elicit distinct privacy protection responses, subsequently influencing self-disclosure in multiple manners.

These conflicting findings suggest a lack of theoretical clarity regarding the role of privacy concerns in shaping self-disclosure on social media, which necessitates further examination. Prior studies on the “privacy paradox” (Barth et al., 2019) have argued that the disconnect between stated privacy attitudes and actual disclosure behaviors challenges the explanatory power of existing privacy decision-making models. Without reconciling these inconsistencies, theoretical frameworks such as the privacy calculus (Dinev & Hart, 2006) risk oversimplifying the cognitive and affective processes underpinning disclosure decisions. As Taddicken (2014) noted, variations in operationalizing privacy concerns and disclosure across contexts can lead to fragmented and non-comparable findings, thereby hindering cumulative knowledge building. By reassessing the relationship between privacy concerns and self-disclosure within a unified and multidimensional framework, this study aims to address this theoretical contradiction and refine the privacy calculus model. If such a clarification is not achieved, the field will continue to lack an integrative theory capable of

explaining divergent empirical outcomes, limiting both the advancement of privacy research and its applicability to evolving social media environments.

Secondly, online privacy is a complex issue, yet most past research tends to focus heavily on a partial perspective. Previous research has primarily focused on individual user characteristics, e.g., privacy concerns and trust (Maqableh et al., 2021; Meier et al., 2021), without adequately explaining how these behaviors are jointly influenced by platform privacy protection mechanisms. Notably, privacy management and self-disclosure are not solely individual issues but are also shaped by privacy features created by platform practitioners.

While some studies have attempted to address this gap by considering privacy protection factors, they often fail to connect these factors with other privacy-related elements critical to individual decision-making. For example, certain studies examine users' concerns or perceived control over risks but overlook how these perceptions, combined with platform assurances, influence disclosure behavior (e.g., Meier et al., 2021; Park & Kim 2020; Cheung et al., 2015). Some studies explore the effects of platform privacy assurance on user behaviors related to trust and information disclosure, but neglect the role of the informational and social environment in shaping self-disclosure (e.g., Kang et al., 2022; Zhu et al., 2022).

In addition, information asymmetry between the online platform and users has been increasingly noticed by scholars (Batoool et al., 2024; Gajewski & Li, 2015; Ivić & Cerić, 2023; Khlifi, 2021). For example, Khlifi (2021) studied the relationship between web-based financial reporting, social media usage, and information asymmetry and found that Twitter, as a channel for information disclosure, has a negative and significant effect on information asymmetry. However, there is limited

research considering how information asymmetry influences users' privacy calculus and self-disclosure in the social media context. Moreover, the regulatory environment also influences individuals' online behavior (Marwala, 2024). For example, Chaudhuri et al. (2023) have shown that government regulation has a significant impact on individuals' online information disclosure. However, few studies have considered building a comprehensive research model to jointly compare the effects of these factors.

To address these gaps, this study identifies four key antecedents, namely individual privacy perception, platform privacy assurance, information asymmetry, and government regulation, that comprehensively influence the privacy calculus and social media self-disclosure.

At the individual level, privacy perception shapes users' subjective evaluation of risks and benefits, reflecting personal awareness and cognition (Gogus & Saygin, 2019). On the platform level, privacy assurance mechanisms, such as privacy settings and privacy policy, mitigate perceived risks and foster perceived security in users' decision-making process (Gong et al., 2019). Information asymmetry between platforms and users further complicates this calculus, as a lack of transparency regarding data collection and usage leads users to overestimate risks and underestimate potential benefits (Khelifi, 2021). Finally, government regulation introduces an institutional safeguard by reducing perceived risks through legal protections (Chaudhuri et al., 2023).

Together, these antecedents provide a comprehensive framework that incorporates individual, platform, transparency, and governmental influences to

further study the influences of these factors on privacy calculus to better understand their relationships to social media self-disclosure.

Thirdly, many studies treat perceived benefits and perceived risks as unidimensional constructs (Liu et al., 2021; Widjaja et al., 2019), ignoring their multifaceted nature. Specifically, the privacy calculus model has been widely used to understand user behavior regarding privacy in digital environments (Gerber et al., 2018). This model posits that individuals make privacy decisions by weighing perceived benefits against perceived risks (Dinev & Hart, 2006). However, many studies treated these two primary components, perceived benefits and perceived risks, as unidimensional constructs. This oversimplification may lead to an incomplete understanding of the complexities involved in users' privacy-related decision-making processes.

Perceived benefits were frequently conceptualized narrowly as functional advantages, such as convenience or enhanced user experience (Meier et al., 2021). However, perceived benefits in privacy calculus were inherently multidimensional and included several dimensions, such as social, emotional, and even psychological factors. For instance, a study by Gerber et al. (2018) highlighted that users derive emotional benefits from self-disclosure on social media, such as feelings of social connectedness or validation. This limited scope fails to capture the holistic nature of the user decision-making process.

Similarly, perceived risks were often treated as unidimensional constructs as well, focusing primarily on the likelihood of privacy breaches or the misuse of personal information (Jozani et al., 2020). However, privacy risks encompass a range of dimensions, including emotional risks (e.g., concerns about the consequences of

privacy breaches), as well as actual consequences of privacy invasion (e.g., reputational risks and the loss of control over personal narratives). Most research overlooked the multidimensional and potentially threatening ways in which risk is perceived. These findings indicate that a more comprehensive approach to the privacy calculus model is essential to address the intricate interplay of factors affecting users decision-making process.

To address these limitations, this study operationalizes perceived benefits and perceived risks as multidimensional higher-order constructs, thereby capturing the broader spectrum of user motivations and concerns. This multidimensional approach allows for a more nuanced understanding of how users weigh benefits and risks, moving beyond the oversimplified trade-off perspective prevalent in earlier research. Methodologically, the use of reflective–formative higher-order constructs within the PLS-SEM framework (Sarstedt et al., 2019) enables the simultaneous assessment of each dimension’s contribution to the overall construct, offering deeper theoretical insights into the complex mechanisms underpinning privacy-related decision-making.

Fourthly, a more comprehensive understanding is needed of how online privacy literacy moderates the connection between privacy calculus and self-information disclosing behaviors on SNS platforms. Only a few studies pointed out the moderating variable in self-disclosure research. Chen et al. (2016) investigated the influence of personality traits on the relationship between social capital and self-disclosure intention and confirmed its moderating role. A study by Lu Yu et al. (2020) demonstrated that the type of online platform plays a significant moderating role in shaping users’ privacy behaviors. Apart from these factors, gender, district, and culture are often tested as moderating variables (Krasnova et al., 2012; Yini Wang et al., 2020; Zhang & Fu, 2020). While these factors, selected from user or platform perspectives,

have been proven to have moderating effects, which also made sense as they widened academic research scope, there is still a need to continue to explore more practical moderating factors to guide the actions of users, platforms, and policymakers.

Masur et al. (2021) indicated that individuals with inadequate media literacy tend to be very subjective and rather arbitrary in their self-disclosure on social media platforms, which makes them more vulnerable when facing privacy invasion. Zhu et al. (2021) claimed that individuals with low privacy information literacy levels tend to generate privacy fatigue, which leads to users putting less effort into making privacy-related decisions and becoming more vulnerable to privacy invasion; Bernadas and Soriano (2019) researched the youth in the Global South, suggesting that online privacy literacy is critical for facilitating online privacy behaviors among poor urban youth. Therefore, improving online privacy literacy education may be a direction worth exploring in the future. Despite its significance being confirmed, research on how online privacy literacy moderates the relationship between users' privacy calculus and self-disclosure is scarce. Thus, this study employs online privacy literacy as the moderating variable to further expand the perspective of self-disclosure in the social media context.

Fifthly, the majority of social media self-disclosure behavior studies were based on Western samples (Bilgihan et al., 2016; Hughes-Roberts, 2013; Oh & Syn, 2015), while the attention paid to non-Western social media users is limited (L. Wang et al., 2020). Conclusions drawn from Western samples may not generally apply to non-Western countries, especially China, for some reasons including individual Internet experiences, mainstream platforms, and cultural norms (Lee et al., 2022; Ying Wang et al., 2020).

The most notable reason is that mainstream social media platforms in China differ from those in most Western countries. In China, popular platforms include WeChat, Weibo, and Douyin, whereas in the West, Facebook, Twitter, and WhatsApp dominate. Although these two sets of platforms have the same basic communication and sharing functions, they differ in privacy features and extended functionalities. For example, WeChat serves as a digital wallet for many Chinese users, integrating payment and financial storage functions, which adds another layer of privacy considerations.

From a cultural perspective, substantial differences exist between Chinese society and Western cultures in terms of privacy conceptualization and disclosure norms. Chinese culture, shaped by collectivist values, often emphasizes relational harmony, face-saving, and trust within in-groups, leading to selective disclosure that is highly context-dependent. In contrast, Western cultures, rooted in individualism, prioritize personal autonomy and self-expression, which can encourage more open and frequent self-disclosure (Acquisti et al., 2015). These orientations translate into specific disclosure patterns: for instance, Americans tend to be more open about sexual topics, whereas Chinese individuals are more willing to share financial information such as income and property values (Acquisti et al., 2015). Similarly, Wang et al. (2011) found that Americans exhibit lower concern about restricting personal information visibility, while Chinese users express heightened concern about identity-related issues on social media.

Given that social media platforms both reflect and reinforce these differences, China's unique sociocultural and technological environment is likely to influence how individuals perceive privacy risks and decide to disclose information online. Therefore, studying the self-disclosure behavior of Chinese users may, to some extent,

fill this empirical gap and deepen our understanding of the factors that influence privacy-related decisions in non-Western contexts.

In summary, while significant progress has been made in understanding privacy calculus and social media self-disclosure, several critical gaps remain, as shown in Table 1.1. Bridging these research gaps is crucial for enhancing both conceptual frameworks and applied knowledge regarding self-disclosure practices in digital social environments.

Table 1.1 The Gap in Prior Studies on Social Media Self-Disclosure

Gap in prior studies	Gap addressed
- Mixed understanding on Privacy concerns; - Partial perception on factors influencing Privacy calculus; - Treat perceived benefits and perceived risks as unidimensional constructs; - Ignore the moderating effect of online privacy literacy; - Mainly focus on Western samples.	- This study conceptualizes privacy concerns as a dimension of perceived risk and explores its association with social media self-disclosure; - This study divides the antecedents of privacy calculus into four aspects and compares the influence of each aspect on privacy calculus; - This study conceptualizes perceived benefits and perceived risks as higher-order constructs with multiple dimensions; - This study employs online privacy literacy as the moderating variable. - This research is mainly conducted in China. The research subjects are Chinese social media platforms and users.

1.4 Research Objectives

The main research objective of this study is to investigate the antecedents of perceived benefits and perceived risks, namely individual privacy perception, platform privacy assurance, information asymmetry, and government regulation, and their relationships with self-disclosure. It further elucidates how online privacy literacy moderates the influence of both perceived benefits and perceived risks on users' information-sharing behaviors in social networking environments. The specific research objectives are as follows.

1. To examine the influence of perceived benefits and perceived risks on users' social media self-disclosure.
2. To examine the associations of individual privacy perception, platform privacy assurance, information asymmetry, and government regulation with perceived benefits and perceived risks.
3. To examine the associations of individual privacy perception, platform privacy assurance, information asymmetry, and government regulation with users' social media self-disclosure.
4. To examine how perceived benefits and perceived risks mediate the relationships of individual privacy perception, platform privacy assurance, information asymmetry, and government regulation to users' social media self-disclosure.
5. To examine how online privacy literacy moderates the relationships of perceived benefits and perceived risks to social media self-disclosure.

6. To examine the most important factor influencing social media self-disclosure.

1.5 Research Questions

This study aims to explore how the perceived benefits and perceived risks, and their antecedents, affect social media self-disclosure behavior. By studying the association of antecedents with perceived benefits and perceived risks of behavior, this study broadens the understanding of the privacy calculus theory and its influence on social media self-disclosure. In addition, this study introduces a moderating variable, online privacy literacy, to explore how it moderates the impact of perceived benefits and perceived risks on social media self-disclosure. This study consists of the following questions.

1. How do perceived benefits and perceived risks influence users' social media self-disclosure?
2. To what extent are individual privacy perception, platform privacy assurance, information asymmetry, and government regulation associated with users' perceived benefits and perceived risks?
3. To what extent are individual privacy perception, platform privacy assurance, information asymmetry, and government regulation associated with users' social media self-disclosure?
4. How do perceived benefits and perceived risks mediate the relationships of individual privacy perception, platform privacy assurance, information asymmetry, and government regulation to users' social media self-disclosure?

5. How does online privacy literacy moderate the relationships of perceived benefits and perceived risks to social media self-disclosure?
6. What is the most important factor influencing social media self-disclosure?

1.6 Scope of the Study

This study is specifically situated in the Chinese context. With the rapid advancement of digital transformation, it is necessary to understand privacy issues and self-disclosure behaviors in China, as one of the largest online markets worldwide. According to the China Internet Network Information Center (CNNIC, 2024), as of June 2024, the proportions of Internet users in China aged 20-29, 30-39, 40-49, and 50-59 were 13.5%, 19.3%, 16.7%, and 19%, respectively. Collectively, these groups accounted for 68.6% of the total internet population, making them the primary demographic for digital engagement. Furthermore, CNNIC (2024) reported that 98% of Chinese internet users are active social media users. Given this, the age distribution of Chinese social media users closely mirrors that of the broader internet population.

Therefore, the participants in this study are Chinese social media users aged 20 to 59. This age range encompasses the majority of the digitally active population, who are heavily reliant on social media for communication, information sharing, and entertainment. This focus ensures that the results can reflect the predominant social media demography in China and offer insights that are widely relevant to major social media users in the nation.

In addition to age considerations, the study is restricted to Chinese social media platforms due to linguistic and cultural factors. Unlike many Western countries where

Western platforms dominate, China's social media landscape is characterized by the widespread use of domestic applications. These platforms have become integral to the daily lives of Chinese users, providing unique ecosystems where users engage in self-disclosure while navigating different kinds of privacy risks and benefits (Wan & Sun, 2023). By focusing on these platforms, this study ensures cultural and contextual relevance, capturing the specific behaviors and preferences of Chinese users in a localized digital environment.

This study focuses on Chinese social media users aged 20 to 59, with an emphasis on domestic platforms such as WeChat Moments, Sina Weibo, and Douyin. By situating the research within this specific context, the study aims to provide more insights into the phenomena of privacy calculus and self-disclosure in one of the world's most dynamic and rapidly evolving digital markets.

1.7 Significance of the Study

Although the relationship between privacy and self-disclosure has been widely studied, research on privacy protection and self-disclosure in social media calls for innovation in light of contemporary developments and varying contexts. This study seeks to address this need by presenting a multidimensional model that enhances the theoretical, methodological, and practical understanding of privacy calculus and self-disclosure in the social media context. The significance of this study is outlined in three aspects: theoretical, methodological, and practical.

1.7.1 Theoretical Significance

This study provides several theoretical contributions to the literature on privacy and self-disclosure. Firstly, the study deepens the theoretical understanding of privacy

decision-making by integrating individual privacy perception into the model. This construct captures users' awareness of privacy and their sensitivity to information disclosure, thereby providing a more comprehensive framework that goes beyond traditional measures of privacy concern. In this way, the study moves the discussion from a narrow risk–benefit calculation to a multidimensional perspective that accounts for how individuals cognitively evaluate privacy in digital contexts.

Secondly, this study enriches the privacy calculus framework by extending its focus from the individual level to a broader contextual perspective. Specifically, this study develops an extended privacy calculus model that incorporates four antecedents—individual privacy perception, platform privacy assurance, information asymmetry, and government regulation. Prior research has examined privacy calculus antecedents in isolation, failing to compare their relative weights and interrelations systematically (Dinev et al., 2013; Kordzadeh et al., 2016). By integrating these four factors, this study provides a comprehensive framework to examine how each antecedent influences perceived benefits and perceived risks and offers a comparative analysis of their relative importance. For instance, individual privacy perception reflects personal concerns and awareness, shaping subjective evaluations of privacy risks and benefits (Kehr et al., 2015). Platform privacy assurance mechanisms, such as privacy settings and privacy policies, are critical in reducing perceived risks (Mousavi et al., 2020; Xu et al., 2011). Furthermore, information asymmetry, a common challenge in digital platforms (Gajewski & Li, 2015), introduces confusion regarding users' understanding of data utilization and collection, making privacy decisions complicated (Khlifi, 2021). Government regulation establishes an institutional safeguard that enhances user security by ensuring legal accountability (Chaudhuri et al., 2023).

Thirdly, this study introduces online privacy literacy as a moderating variable in the relationship between privacy calculus and self-disclosure. While online privacy literacy has been shown to influence users' privacy-related decisions (Bartsch & Dienlin, 2016), its role as a moderating variable in self-disclosure research remains underexplored. By examining its moderating effects, this study aims to bridge this gap and extend the theoretical understanding of how privacy literacy can shape privacy behaviors.

1.7.2 Methodological Significance

Methodologically, this study employs advanced techniques-structural equation modeling (SEM) using SmartPLS software. The two-step approach employed in this study allows for a comprehensive analysis of measurement and structural models (Hair et al., 2021). Additionally, the study introduces novel analysis methods, including the marker variable technique to detect common method bias, importance-performance map analysis (IPMA) to test antecedents' importance and performance score, and model comparison to assess the alternative model.

In order to expand the analysis methods in self-disclosure research, this study developed four higher-order constructs (HOC) based on the literature review, namely individual privacy perception, platform privacy assurance, perceived benefits, and perceived risks. These constructs are all of the reflective-formative type, namely Type II according to Sarstedt et al. (2019). The measurement model analysis of these four constructs should be distinguished from the reflective constructs. In addition, when conducting structural model evaluation, the indicators of high-order constructs come from the latent scores of their lower-order constructs (LOC). These will be explained in detail in Chapter 3. The use of reflective-formative higher-order constructs is rare