Volume 1, 2025, Pages 41-49 *Elaris Computing Nexus*
| Regular Article | Open Access

A Structural Equation Modeling Approach to Understanding Privacy Concerns Reliability and Self Disclosure on Facebook

Sungsoo Song
Wonkwang Health Science College, Iksan-si, Jeonbuk State, South Korea.
sungsoo586@hotmail.com

Article Info
Elaris Computing Nexus
https://elarispublications.com/journals/ecn/ecn_home.html

https://doi.org/10. XXXX/ECN/2025005

Received 06 March 2025
Revised from 18 April 2025
Accepted 22 April 2025
Available online 06 May 2025
Published by Elaris Publications.

Corresponding author(s):
Sungsoo Song, Wonkwang Health Science College, Iksan-si, Jeonbuk State, South Korea.
Email: sungsoo586@hotmail.com

Abstract – The study examines the interplay between privacy concerns, privacy management, self-disclosure, reliability, and the importance of addressing privacy in online social networks, using Facebook as a case study. We provide a detailed structural equation model (SEM) to assess the direct and indirect impacts of privacy-related factors on user behavior. A survey of 500 active Facebook users was conducted online, and the resulting dataset was purified to exclude missing values and issues with insufficient variable loading. The assessment models were assessed for reliability by AVE (average variance extracted), CR (composite reliability), and Cronbach's alpha, while the structural analysis was scrutinized for multicollinearity and outliers. The results demonstrate that data risk substantially influences reliability in self-disclosure, privacy, and Facebook. Reliability significantly influences privacy concerns, self-disclosure, and privacy management on Facebook.

Keywords – Privacy Issues, Privacy Control, Self-Disclosure, Reliability, Confidentiality, Structural Equation Modeling, Online Social Networks, Facebook, User Behavior.

I. INTRODUCTION

The emergence of the Internet and social media has profoundly altered every facet of our existence, including our work, consumption, and communication. Although this has provided significant benefits to society, the increasing impact of the Internet and technology has consistently raised issues around confidentiality and the gathering and usage of personal data. The risks to personal privacy posed by these advancements have been extensively recorded. In recent years, sensitive data has been fraudulently acquired and improperly managed in many data breaches. Over the past few decades, between May and July 2017, sensitive personal data, such as credit scores, of approximately 147.9 million Americans were exposed in the American credit bureau Equifax breach. In addition, in 2018, confidential data belonging to approximately 87 million Facebook users was inappropriately shared with the with Cambridge Analytica [1].

Social networks facilitate the creation and participation in groups with varied interests via the generation of private sites that include demographic information. Community membership is seen as a valuable resource for information-gathering activities. Filho and O'Neale [2] provide innovative metrics, including diffusion and monopoly factors, to enhance bipartite structures, especially with community overlap. The two metrics are used to discern intricate patterns inside real social networks. Unwanted disclosure of user information will be disseminated on online social networks (OSN). The personal and professional aspects of user life facilitate incidents with severe repercussions. Anonymous data analytics used during de-anonymization and characterization result in user security breaches. The substantial amount of private information, either inadvertently disclosed by typical users or owing to the deficiency of advanced privacy features in OSNs, has driven several firms to aggregate and sell social media data to other entities or individuals.

Even though social media sites provide new options for connection and automatic data transmission, privacy and security have become a major issue within these landscapes. A privacy breach happens when an intruder gains unauthorized accessibility to a site's protected written information or codes. Privacy issues, such as those related to unlicensed access to

confidential data, may not fundamentally integrate privacy breaches. Confidential information may be accessed by only seeing a person input their password. Both clusters of violations often intersect on social networks, certainly when individuals compromising a site's privacy facilitates accessibility to privacy information of any individual. In reality, users tend to disregard or neglect privacy and security concerns linked to OSNs.

Personal data on people is now accessible to the public in an unparalleled manner and scale, including vast amounts of digital images and videos. Individuals may lose control over the use of their data after it is disseminated over the network. User conversations may be recorded forever, searchable, replicable, and modifiable, and may be accessible by others without the participants' awareness. Disseminating one's personal data may indeed make it accessible to an entire subscriber community. Presently, minor protective measures are applied to prevent unpermitted replication of personal data from profiles for creating individual profiles or redistributing the data elsewhere.

A growing concern regarding online social networks is the matter of privacy and its impact on user behavior. The heightened sharing of personal information on social media platforms like Facebook prompts an inquiry into the interplay of privacy, self-disclosure, reliability, and privacy management in shaping the essence of privacy and self-disclosure management. This research aims to explore these interactions with SEM to provide a comprehensive understanding of how privacy constructs influence user behavior in different OSNs.

The remaining sections of this study have been arranged in the following manner: Section II provides a review of related work and theoretical background on OSNs vulnerabilities, privacy/reliability in OSNs, SEM in privacy research, and consumer privacy concern. Section III describes the methodology employed in our study, and highlights our (i) data collection and variable screening method, (ii) measurement model and reliability assessment, and (iii) structural model evaluation and hypothesis testing. Section IV and V provides a discussion of our findings, emphasizing on structural model evaluation; and model fit and path analysis. Section VI concludes the study and highlights the significant effects of data risks and reliability on privacy concern, as well as user behaviors.

II. RELATED WORK AND THEORETICAL BACKGROUND

Vulnerabilities in OSNs

Although significant issues exist regarding the security of OSNs (e.g., ensuring proper formatting of profiles and devoid of browser activities, mitigating denial-of-service (DoS) attacks), Pan et al. [3] investigate threats related to the quality of data accessible via OSNs, even when the foundational architecture is protected (see **Table 1**).

Table 1. Vulnerabilities related to quality of data access in OSNs

Threat Type	Description	Examples/Implications	Ref.
Malicious Infiltration	Social networks provide an illusion of privacy but can be infiltrated by malicious users.	Observed on MySpace and Facebook	[4]
Nearby Threats	Users control direct friends, but threats can come from distant connections due to the small world effect.	Rogue profiles on MySpace with hundreds of connections.	[5]
Limited Network View	Users can't see or control the entire network, leaving unknown risks from other members.	Users can't fully monitor or control all network members.	[6]

As described by Buchanan and Benson [7], malicious individuals might use the apparent social connections among users to enhance the likelihood of spreading disinformation, directing participants to nefarious corners of the Web (e.g., websites harboring malware), and causing other issues to the integrity of community-centric knowledge. To mitigate these weaknesses, we may use many strategies, such as background investigations, legal enforcement, and dependence on a reputable centralized authority. A purely legal strategy is used by several prominent social networking platforms, whereby users detected as violating the conditions of service can be excluded from the networks.

A trustworthy central agency can be authorized to oversee the online community, similar to Facebook and MySpace. Also, users may need to complete background screening to provide offline guarantees of their quality. These methodologies often encounter issues related to enforcement and scalability.

Privacy and ReliabilityiIn Osns

A study by Finska, Hakkala, and Majanoja [8] indicates that personal data of more than 100,000 OSN influencers was breached and partly disclosed due to an intrusion at a social media marketing firm. In addition, investigations show that due to this security attack, an additional 250,000 users have had their data completely compromised on the dark web. They indicated that 80% of users expressed apprehension over online marketing and companies accessing their data on OSNs. Furthermore, 74% of users consider it crucial to maintain control over accessibility of personal data.

Ho, Maiga, and Aimeur [9] indicated that privacy is a primary issue for users of social networking platforms. They argued that users of social networking platforms perceive a lack of control over their privacy. They also examined the primary data risks associated with social media, which included data collection, secondary use, inaccuracies, unauthorized access, control, and user awareness. The issues originated from prior research conducted by Young and Quan-Haase [10], which

examined Internet privacy. They characterized privacy issues as "the extent to which a user is apprehensive about site's protocols pertaining to the gathering and utilization of their private data."

SEM in Privacy Research

According to Fitzgerald et al. [11], the application of formal validation techniques is essential for solidifying fundamental concepts in prominent IS research domains, including Structural Equation Modelling (SEM) and Multi-Trait Multi-Method (MTMM) analysis. Among SEM methodologies, Partial Least Squares Structural Equation Modeling (PLS-SEM) is a prominent aspect of data analysis within the domain of Information Systems (IS), including Behavioral Information Security (BIS). In information security, BIS denotes "the activities undertaken by users that influence the integrity, confidentiality, and availability of IS", a perspective that posits that technological solutions alone are insufficient to address the challenges of data security. Research on privacy and openness on SNSs (social networking sites) belongs to that area.

As the utilization of PLS-SEM has escalated among researchers, Bayaga and Kyobe [12] suggested methodologies for implementing this technique. The authors used the investigative aspect of their work (14%) to rationalize the application of theory, PLS-SEM, and model evaluation (10%). Ultimately, the rationale behind PLS-SEM's superior performance compared to older classical regression approaches accounts for 10%. In all, 29% of the investigations, including 6 articles, failed to provide any rationale for using PLS-SEM. An overview of these considerations is provided in **Table 2**.

Table 2. Overview of the rationale for selecting PLS-SEM.

PLS-SEM benefits	F (n = 21)	% (5)
Small sample volume	7	33
Nonparametric data	5	24
The ability to manage intricate (analytical) frameworks	5	24
The exploratory character of the research	3	14
Exceeds the efficacy of conventional Ordinary Least Squares (OLS)	2	10
PLS optimizes the endogenous constructs' variance.	1	5
Increased effectiveness in parameter estimation	1	5
Statistical energy	1	5
Model/Hypothesis testing	2	10
Permits a thorough examination of the links between	1	5
Not mentioned	6	29

Consumer Privacy Concerns

As argued by Culnan and Bies [13], consumer privacy is often defined by researchers as the capacity of an individual to regulate the timing, manner, and degree of dissemination of their personal information to other parties. They examined the correlation between privacy concerns and several factors, such as customer attitudes and behaviors.

Consumer privacy concerns have emerged as a significant problem after the Facebook–Cambridge Analytica data breach, 2018, during which Cambridge Analytica illicitly capture confidential data from 87 million Facebook users without permission for political reasons. Furthermore, Facebook disclosed further data breaches, including a software vulnerability that potentially exposed the postings of around 14 million users and a security breach that enabled an unidentified entity to commandeer 50 million accounts.

According to Baker and Kim [14], service failures often result in a detrimental experience for customers. Research on service failure and recovery has advanced significantly over the last thirty years, yielding substantial insights into how companies can address service failures. In a study of 44 empirical studies, they determined that most research has focused on recovery techniques, including apology and explanation, as well as the impact of compensation on customer responses.

Nonetheless, there is a lack of actual evidence from impacted consumers about the periods before, during, and after a service breakdown. Research examining pre- and post-service failure is often conducted in a simulated laboratory setting. A void exists in the research on the long-term effects of service failure, particularly with customer protective behavior.

III. METHODOLOGY AND HYPOTHESIS

In this paper, we will explore the linkages between core concepts within the environment of OSNs, especially the links between confidentiality, reliability, privacy control, self-disclosure and privacy concerns. SEM, which is an extensive statistical tool, is used to test the research model by considering the intricate relation among the latent and the observed variables. Such a method is effective in evaluating the structural and measurement model to enable identifying the direct and indirect effects in the hypothesized model.

Data Collection and Variable Screening

Information was gathered in an online survey which is circulated among active Facebook users. The analysis of the final sample including 500 respondents focused on the privacy concerns of the users of the platform, self-disclosure behaviors, and reliability in the platform. The data were first checked to determine whether any data were missing, and data were imputed, using Expectation-Minimization (EM) algorithm.

A follow-up screening of variables was done to remove the variables that failed the screening requirements of inclusion. Variables with factor loading (FL) lower than 0.5 were not included in the model as it is considered the weak indicator on the underlying constructs. To be particular, five variables were deleted: SD5 (Self-disclosure construct), PCt3 and PCt4 (Privacy control construct), CF1 (Confidentiality construct), and RL4 (Reliability construct). After removal of these variables, 19 items were left to be analyzed further.

Measurement Model and Reliability Assessment

Cronbach alpha, which is a reliability measure of consistency used worldwide, was used to test the measurement model. The values of Cronbach alpha of concepts in the final model were between 0.772 and 0.901, indicating good reliability. The FLs were assessed to measure the convergent validity. The findings revealed that the rest of the items had sufficient loadings indicating that the items that belonged to each construct were tightly associated to the latent construct. The factor loading analysis was repeated until the pattern of factor loading observed was cleaner and may be said to confirm the reliability of the measurement framework.

Moreover, a confirmatory factor analysis (CFA) was conducted to evaluate the match of the measurement framework. The fit statistics such as RMSEA (root mean square error of approximation), NFI (normed fit index) CFI (comparative fit index), and GFI (goodness-of-fit index) were addressed. All indices were within ideal threshold values and this suggests that the model fitted the data properly. AV (average variance extracted), CR (composite reliability) were also analyzed to test the framework validity and reliability. All CR values were more than the minimum acceptable (0.7) and AVE ranged between 0.587 and 0.689, exceeding the suggested minimum (0.5), which indicates both discriminant and convergent validity.

Model/Hypothesis Testing

After the measurement framework was rated, its structural framework has been evaluated. The first stage to be used was a multivariate analysis that was first applied to determine the possible presence of an outlier based on Cook range. Abnormal range of Cook was removed in cases. Subsequently, the presence of multiple correction was checked using Variance Inflation Factor (VIF) where the values were all within the 1 to 4 range, indicating the occurrence of multicollinearity was non-existent.

The main purpose surrounding the structural framework analysis was to test the hypotheses holding the connections between the independent variables (data risk, reliability, and confidentiality) and the dependent variable (privacy concern). In this regard, the model should also be evaluated in terms of the relations between privacy concern and the issues of privacy control and self-disclosure. The findings showed that the independent variables explained privacy link to 46.4 percent in the model, which is sufficient enough to show their influence. It was found that reliability on Facebook has a statistically significant implication on the self-disclosure and privacy control with a coefficient of -0.284 and 0.355 respectively. All the paths among the constructs showed up as significant at $p < 0.001$ with t-values considerably greater than the critical threshold of 2.0, which further elucidates the soundness of the model.

All the relationships between data risk to reliability, and privacy issue, confidentiality, reliability and the other constructs were as postulated, showing the importance of these concepts on the user conduct. The outcomes imply that the likelihood of data risk considerably affects reliability in Facebook (beta = - 0.413), privacy concern (beta = 0.627), and confidentiality has a moderate effect on the privacy concern (beta = 0.231). This reliability has a significant impact on self-disclosure and concern, privacy as well as privacy control in a standardized coefficient of 0.355, -0.274, and -0.284, respectively.

According to the theoretical framework, the study proposes the following hypothesis:

- H1: Data risk substantially affects reliability in Facebook.
- H2: Data risk substantially influences privacy concern.
- H3: The value of privacy considerably affects privacy concerns.
- H4: Reliability in Facebook significantly influences privacy control.
- H5: Reliability in Facebook markedly affects self-disclosure.
- H6: Reliability in Facebook substantially affects privacy concerns.

The hypothesis was tested using route analysis and the results indicated that, all the assumed linkages were statistically significant, therefore justifying the predictability of the hypotheses. The results advance knowledge on the multidynamic interplay between both privacy issues, self-disclosure, and reliability in social media contexts, which is of great importance to future research, and field applications in privacy management and online behavior.

IV. RESULTS

The data were analyzed using AMOS 23.0 software, and IBM's SPSS Statistics 23.0 tools. We evaluated our hypothesis with SEM.

Structural Model Evaluation

Upon examining each variable for absent data, we conducted FLs analysis and iterated the process until achieving an error-free pattern matrix. Variables with loadings below 0.5 were excluded, specifically SD5 (Construct 5 for Self-disclosure), PCt3 (Construct 3 for Privacy control), CF1 (Construct 1 for Confidentiality), and RL4 (Construct 4 for Reliability). Consequently, our model comprised a total of nineteen items.

We assessed convergent validity using Cronbach's alpha (α), a widely used metric that evaluates the degree to which several items for a concept are interrelated. The coefficient fluctuates between 0 and 1. In our study model, α varied from 0.772 to 0.901. The satisfactory reliability coefficient is over 0.7, but other writers assert that it may be beyond 0.6 during exploratory study. α was computed for every hypothesis, using all objects remaining after the segregation of five elements. **Table 3** provides a summary of all values.

Table 3. FLs with α

Construct Category	Item(s)	Factor Loading(s)	No. of Items	Cronbach's α
Data risk	DR1, DR2, DR3	.824, .852, .603	3	.800
Confidentiality	CF2, CF3	.452, .484	2	.772
Reliability in Facebook	RL1, RL2, RL3	.843, .726, .770	3	.824
Self-Disclosure	SD1, SD2, SD3, SD4	.775, .858, .789, .608	4	.851
Privacy Control	PC1, PC2	.987, .683	2	.788
Privacy Concerns	PCs1, PCs2, PCs3, PCs4, PCs5	.756, .902, .755, .714, .834	5	.901

The final components of our model's FLs are illustrated in **Table 3**. The results indicate the study instrument's dependability, shown by its elevated FLs and substantial internal consistency. The model factor was then submitted to a confirmatory analysis. The initial measurement model's fit to the data is shown in **Table 4**. We have presented four fit indices: Normed Fit Index (NFI), Goodness-of-Fit (GFI), Comparative Fit Index (CFI), and Root Mean Square Error of Approximation (RMSEA). The values proposed in the Table were altered from those in [15]. No value exists beyond the parameters deemed ideal.

Table 4. The findings of the measurement model fit test are satisfactory

Model Criteria	Measurement Model	Recommended Value
RMSEA	.074	≤ .10
NFI	.903	≥ .90
CFI	.923	≥ .90
GFI	.903	≥ .90

Table 5 presents the CR, AVE, and the component correlations matrix, which demonstrate the reliability and validity of our framework. The CR figures above the minimal threshold of 0.7, ranging from 0.864 to 0.944. The retrieved AVE values vary from 0.587 to 0.689, with a minimum threshold of 0.5, all above the suggested minimum value. The AVE value surpasses the squared correlation across several hypotheses, hence validating the criterion for discriminant validity. All constructs exhibit strong discriminant validity, as seen in **Table 5**. In conclusion, our model exhibits no issues with validity or reliability.

Table 5. CR, AVE, and the matrix of component correlations.

Model Criteria	Data risk	Confidentiality	Reliability in Facebook	Self-Disclosure	Privacy Control	Privacy Concerns
CR	0.881	0.864	0.893	0.910	0.883	0.944
AVE	0.587	0.642	0.615	0.594	0.689	0.654
DR	0.766	0.314	0.130	0.047	0.020	0.401
CF	0.314	0.801	0.003	0.041	0.003	0.215
RL in Facebook	0.130	0.003	0.784	0.062	0.228	0.157
SD	0.047	0.041	0.062	0.771	0.001	0.015
PC	0.020	0.003	0.228	0.001	0.830	0.031
PCs	0.401	0.215	0.157	0.015	0.031	0.809

The highlighted diagonal components denote the square root of AVE. Initially, we conducted multivariate assessments for end values and important observations using Cook's distance technique. Three examples had anomalous Cook's distances, prompting their removal during the structural evaluation step. A multiple correlation assessment was conducted using the VIF (variance inflation factor) that is expected to fall between 1 and 4, and all findings adhered to this range. Subsequently, theories were evaluated using the pathways.

Model Fit and Path Analysis

Our framework was evaluated for overall fit and for individual path assessments. **Fig. 1** shows the outcomes of the path assessment concerning the relationships among different groupings of components.

The R^2 value in the framework indicates the extent to which dependent variables are elucidated by independent variables. In this framework, privacy concerns are elucidated by 46.41% through reliability, confidentiality, and data risk in Facebook. This indicates that over 50% of the construct of privacy issue is elucidated by the framework proposed in this research. Reliability in Facebook accounts for 6% of self-disclosure and 22% of privacy management. Reliability in Facebook is attributed to data risk at a rate of 11.82%. In our prior study, privacy issues accounted for 38.11% of the variance, whereas

self-disclosure was emphasized, explaining 32.6% of the variance. our finding emphasizes our concentration on the privacy issues constructed inside our model, which was significantly elucidated by the independent variables involved.

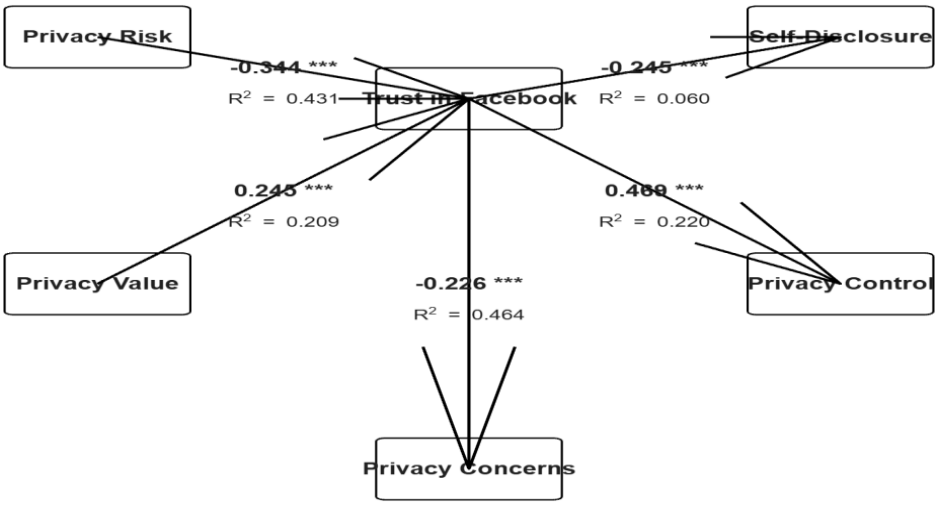

Fig 1. The Examination of Route Coefficients

The hypotheses are clarified by looking at the route coefficients and the t-test results. Each pathway's significance and resilience are assessed with a t-value and standardized coefficient (β), which ought to be greater than 2.0 or less than −2.0. **Table 6** displays the results of the hypothesis testing and path evaluation. All t-statistic values either exceeded 2.0 or fell below −2.0, and all routes in our framework had p values below 0.001, indicating statistical significance.

Table 6. Findings of hypothesis testing

H	T-Statistic	Standardized Coefficient β	Path	The Result
1	-6.851	-0.413 ***	PR - RL	Accepted
2	7.711	0.627 ***	PR - PCs	Accepted
3	4.118	0.231 ***	CF - PCs	Accepted
4	-5.183	-0.284 ***	RL - SD	Accepted
5	7.528	0.355 ***	RL - PCt	Accepted
6	-5.525	-0.274 ***	RL - PCs	Accepted

*** $p < 0.001$.

Data risk substantially impacts confidence in Facebook, with privacy issues exhibiting consistent values of 0.627 and −0.413, and t-statistics values of −6.0 or 7.0, respectively. The value of privacy exerts a substantial influence, with a β of 0.230 and t-statistics values above 4.01 regarding privacy issues. RL significantly influences PCs, PC, and SD, with Z-score −0.274, 0.355, and −0.284, correspondingly, and t-statistics values above −5.0 and 7.0. All implications are substantial and can be addressed in the subsequent section.

V. DISCUSSION

Facebook and other online social networks are integral to the daily lives of many individuals. Users of online social networks disseminate substantial amounts of personal data daily. The proliferation of online social networks has introduced new challenges regarding users' perceptions of SD, RL, and CF.

The data leaking of social network users poses a significant hazard. Wang, Chen, and Atabakhsh [16] presented several methods for identity collection, cloning, and their application in criminal activities. An identity theft attack results in the breach of user privacy. The email ID serves as the sole novel identifier that may lead to the revelation of additional information. Three strategies for mitigating Identity Theft attacks are discussed in [17]. The revelation of one's location constitutes a serious privacy concern. Smartphones offer cutting-edge Internet connectivity, supplemented by location data derived from GPS and Internet-based sources. These smartphones also offer upgraded social networking applications with actual data sharing and connectivity. Mobil share infrastructure is implemented to resolve location allocation issues in mobile online social networks (mOSNs). Enhancements are proposed in the collection of location information.

Authors presented the classification of trusted and untrusted data services providers and recommended the application of the k-anonymity method for data disclosure. Users rely on online social networks for interaction inside their groups. The fundamental four factors that attract spammers are (i) the governing entity of the whole OSN, (ii) clearly defined communications, (iii) user identity, and (iv) many OSN interfaces offering diverse perspectives. Spam is disseminated on online social networks to gather user actions and data, resulting in privacy breaches. Conventional and technology coping strategies are proposed to safeguard against identity theft in [18].

Our study aimed to construct a model illustrating how the statistical value of privacy and apparent data risk influence users' consistency in OSNs, self-disclosure, confidentiality issues, and confidentiality control inside these platforms. This

study's model was constructed based on prior study in the domains of Disclosure, Reliability, and Privacy. Online information gathering techniques were employed to authenticate our framework. The survey included 602 participants aged 18 to 63, all of whom utilize Facebook and reside in Slovenia.

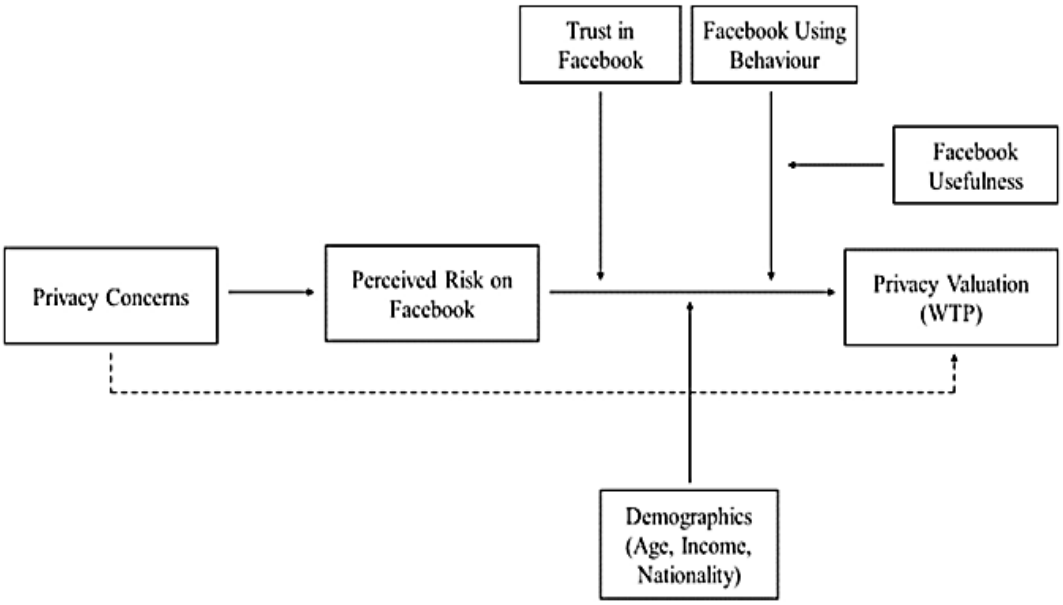

Fig 2. Hypothetical Framework Supporting Privacy Assessments

Our findings supplied the framework with 6 constructs: self-disclosure, privacy issues, privacy control, dependability in Facebook, data risk, and confidentiality. These were evaluated on Facebook users. The preliminary measurement framework was constructed, subsequently examined, and refined into the final test framework. SEM assessment has validated the final study model, with 5 of the 6 tested hypotheses corroborated by the route analysis results. In our approach, data risk and confidentiality are independent entities, both positively influencing privacy concerns, whereas data risk negatively affects Facebook reliability. The Facebook reliability mediator directly influences the constructs of PC, PCs, and SD.

The importance of privacy positively influences privacy concerns. This influence indicates that an increased valuation of privacy by the user correlates with heightened privacy concerns. Xu, Michael, and Chen [19] presented a theoretical model delineating the anticipated correlations among psychological variable quantity in forecasting Web users' privacy assessments on OSNs (refer to **Fig. 2**). The selected psychological characteristics are based on previous work indicating their significance in the realm of data privacy. Psychological assessments are modified as needed to align with the setting of Facebook. Facebook perceived risk mediates the link between privacy valuation and privacy concerns, and that this link is further qualified by the degree of reliability in Facebook and Facebook use, and its Data Standards. We assert that elevated privacy concerns forecast a greater inclination to pay for confidentiality, intermediated by heightened perceptions of privacy-related risks on Facebook. Privacy valuation is anticipated to rely on the present usage of Facebook by its members or the perceived utility of Facebook by non-members, respectively. Recurrent Facebook users with heightened privacy issues are anticipated to demonstrate a stronger inclination to spend for privacy on the platform compared to those with diminished privacy worries.

Facebook’s non-members who harbor significant privacy issues and view Facebook as beneficial are anticipated to demonstrate a greater readiness to spend for privacy compared to those non-members who do not regard Facebook as significant. The reasoning is that those troubled about privacy, who view Facebook as beneficial yet do not join the platform, may refrain from participation owing to privacy apprehensions rather than a lack of perceived advantages, making them more inclined to invest in privacy on Facebook. Alongside these emotional traits, socio-demographic data and the psychological attributes of comparative optimism and social norms will also be evaluated, since they may provide supplementary descriptive energy beyond the key model variables.

Confidence in Facebook was determined to adversely impact self-disclosure on the platform. We expected that confidence in Facebook would negatively affect self-disclosure; nevertheless, other studies have indicated a beneficial effect. The negative trajectory was identified in [20], whereas other investigations corroborated its favorable influence. The assumptions of the SIDE model, as previously discussed in the hypothesis formulation, may elucidate the adverse effect, as heightened salience of an individual's social identity correlates with increased reliability and self-disclosure.

Confidence in Facebook positively influences privacy control while negatively affecting privacy concerns. Additional studies have similarly identified a substantial negative correlation between Facebook’s privacy issues and reliability, and we did not see any other research examining the relationship between reliability in privacy control and website usage. These hypotheses suggest that more confidence in Facebook correlates with greater information disclosure and diminished privacy concerns. The user will perceive an enhanced sense of privacy control with increased reliability in Facebook.

The findings of our study on self-disclosure, reliability, and privacy in OSN align with prior studies in most cases and provide a novel model with strong overall fit. The findings provided new insights into the research about reliability development on Facebook, privacy restrictions and issues, and self-disclosure on OSNs. While certain pathways have been established in prior research, this model has not previously been constructed, hence offering novel insights into users' perceptions of self-disclosure, reliability, and privacy on Facebook. The methodology enhances researchers' comprehension of connections across many characteristics and can be implemented across other platforms, not exclusively on OSNs.

The model assists OSN developers in comprehending user sentiments regarding privacy and the circumstances in which they share the most information, likely aligning with the objectives of OSNs. To maximize the use of this framework, we have established the detrimental effect of RL on SD by means of the SIDE framework as a foundational model, and we have also identified a highly substantial relationship between privacy control and reliability that has not been previously examined.

VI. CONCLUSION

SEM analysis has demonstrated the substantial influence of data risk and reliability on privacy concerns and user behavior. The results demonstrate that data risk influences privacy issues and reliability in Facebook, but confidentiality impacts concerns over personal privacy. Furthermore, reliability has become a pivotal element influencing privacy management, self-disclosure, and privacy apprehensions. The findings highlight the presence of reliability-enhancing processes in online social networks that alleviate privacy concerns and promote responsible self-disclosure. The study highlights the importance of advanced privacy management solutions that allow users to control their sensitive data, hence promoting a more secure and transparent environment. The results correspond with the growing body of literature on privacy in online social networks and offer practical significance for platform developers, policymakers, and future research in the field of digital privacy.

CRediT Author Statement

The author reviewed the results and approved the final version of the manuscript.

Data Availability

The datasets generated during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interests

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Funding

No funding was received for conducting this research.

Competing Interests

The authors declare no competing interests.

References

[1]. V. Chergarova and L. Wang, “Falsifying Personal Data To Address Online Privacy Issues,” Issues in Information Systems, Jan. 2019, doi: 10.48009/2_iis_2019_183-194.
[2]. D. V. Filho and D. R. J. O’Neale, “The role of bipartite structure in R&D collaboration networks,” Journal of Complex Networks, vol. 8, no. 4, Apr. 2020, doi: 10.1093/comnet/cnaa016.
[3]. T. Pan et al., “Threat from Being Social: Vulnerability analysis of social Network coupled Smart Grid,” IEEE Access, vol. 5, pp. 16774–16783, Jan. 2017, doi: 10.1109/access.2017.2738565.
[4]. C.-H. Chang and M. Potkonjak, Secure system design and trustable computing. 2015. doi: 10.1007/978-3-319-14971-4.
[5]. M. Fire, R. Goldschmidt, and Y. Elovici, “Online social networks: Threats and solutions,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019–2036, Jan. 2014, doi: 10.1109/comst.2014.2321628.
[6]. C. Liang and F. R. Yu, “Wireless Network Virtualization: A survey, some research issues and challenges,” IEEE Communications Surveys & Tutorials, vol. 17, no. 1, pp. 358–380, Aug. 2014, doi: 10.1109/comst.2014.2352118.
[7]. T. Buchanan and V. Benson, “Spreading disinformation on Facebook: Do trust in message source, risk propensity, or personality affect the organic reach of ‘Fake news’?,” Social Media + Society, vol. 5, no. 4, Oct. 2019, doi: 10.1177/2056305119888654.
[8]. K. Finska, A. Hakkala, and A.-M. Majanoja, “Security and privacy enhancing framework for Social Media Influencers and Content Creators,” CompSysTech ’24: Proceedings of the International Conference on Computer Systems and Technologies 2024, pp. 37–42, Jun. 2024, doi: 10.1145/3674912.3674942.
[9]. Ho, A. Maiga, and E. Aimeur, “Privacy protection issues in social networking sites,” 2009 IEEE/ACS International Conference on Computer Systems and Applications, pp. 271–278, Jan. 2009, doi: 10.1109/aiccsa.2009.5069336.
[10]. L. Young and A. Quan-Haase, “Privacy protection strategies on Facebook,” Information Communication & Society, vol. 16, no. 4, pp. 479–500, Apr. 2013, doi: 10.1080/1369118x.2013.777757.
[11]. Fitzgerald, K.-J. Stol, R. O’Sullivan, and D. O’Brien, “Scaling agile methods to regulated environments: An industry case study,” 2013 35th International Conference on Software Engineering (ICSE), pp. 863–872, May 2013, doi: 10.1109/icse.2013.6606635.
[12]. Bayaga and M. Kyobe, “PLS-SEM technique and phases of analysis – implications for information systems’ exploratory design researchers,” 2021 Conference on Information Communications Technology and Society (ICTAS), pp. 46–51, Mar. 2021, doi: 10.1109/ictas50802.2021.9395029.
[13]. M. J. Culnan and R. J. Bies, “Consumer Privacy: Balancing economic and justice considerations,” Journal of Social Issues, vol. 59, no. 2, pp. 323–342, Apr. 2003, doi: 10.1111/1540-4560.00067.
[14]. M. A. Baker and K. Kim, “Other customer service failures: emotions, impacts, and attributions,” Journal of Hospitality & Tourism Research, vol. 42, no. 7, pp. 1067–1085, Oct. 2016, doi: 10.1177/1096348016671394.

[15]. K. Lai and S. B. Green, "The Problem with Having Two Watches: Assessment of Fit When RMSEA and CFI Disagree," Multivariate Behavioral Research, vol. 51, no. 2–3, pp. 220–239, Mar. 2016, doi: 10.1080/00273171.2015.1134306.
[16]. G. Wang, H. Chen, and H. Atabakhsh, "Criminal Identity deception and deception detection in law enforcement," Group Decision and Negotiation, vol. 13, no. 2, pp. 111–127, Mar. 2004, doi: 10.1023/b:grup.0000021838.66662.0c.
[17]. F. Lai, D. Li, and C.-T. Hsieh, "Fighting identity theft: The coping perspective," Decision Support Systems, vol. 52, no. 2, pp. 353–363, Sep. 2011, doi: 10.1016/j.dss.2011.09.002.
[18]. T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao, "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," Information Systems Journal, vol. 24, no. 1, pp. 61–84, Jul. 2012, doi: 10.1111/j.1365-2575.2012.00420.x.
[19]. F. Xu, K. Michael, and X. Chen, "Factors affecting privacy disclosure on social network sites: an integrated model," Electronic Commerce Research, vol. 13, no. 2, pp. 151–168, Mar. 2013, doi: 10.1007/s10660-013-9111-6.
[20]. W. J. Bingley, K. H. Greenaway, and S. A. Haslam, "A Social-Identity Theory of Information-Access Regulation (SITIAR): Understanding the psychology of sharing and withholding," Perspectives on Psychological Science, vol. 17, no. 3, pp. 827–840, Oct. 2021, doi: 10.1177/1745691621997144.