JOURNAL OF MASS COMMUNICATION JMCD
Vol. 34, May 2026 | www.jmcd-uok.com

Privacy Risks and Online Self-Disclosure: Examining Privacy Invasion Experience and Privacy Control among Pakistani University Students

Muhammad Usman[1] & Dr. Sana Shahid[2]

Abstract

Online self-disclosure has become a central feature of digital communication, yet it remains shaped by complex evaluations of perceived risks and contextual influences. This study examines privacy invasion experience impact on online self-disclosure among university students in Pakistan, while also evaluating moderating role of privacy control. Drawing on Privacy Calculus Theory and Communication Privacy Management Theory, study employs a quantitative design using survey data from 443 students and analyzes relationships through PLS-SEM. Findings reveal that privacy invasion experience significantly influence online self-disclosure in shaping digital behavior, however, privacy control does not significantly moderate these relationships. Study contributes to literature by extending privacy calculus through experiential privacy-related risk dimensions and provides insights for developing safer and more context-sensitive digital environments.

Keywords: Online self-disclosure; perceived risks; privacy invasion experience; privacy control

Introduction

Fast development of digital media has fundamentally altered pattern of human communication, shifting it to both networked and platform-mediated environments (Ayub et al., 2024; Jones, 2013; Deuze and McQuail, 2020). Advancement of social networking sites like Meta Platforms Facebook, ByteDance TikTok, and WhatsApp LLC has normalized practice of constant information sharing, where users can disclose personal thoughts, experiences, and identities to a large audience and often unknown audiences (Dolan et al., 2019; Malhan et al., 2021).

[1]Muhammad Usman, Ph.D. Scholar, Department of Media & Communication Studies, SMIU Karachi, usman4162002@gmail.com
[2]Dr. Sana Shahid, Assistant Professor, Department of Media & Communication Studies, SMIU, Karachi, sana@smiu.edu.pk

Online self-disclosure has become one of crucial processes in relationship-building, identity-construction, and socialization process (Bazarova and Choi, 2014; Davis, 2012; Schlosser, 2020).

Online self-disclosure, which is voluntary disclosure of personal information in online setting, is markedly different compared to offline interaction owing to anonymity, synchronicity and diversity of audience (Hollenbaugh, 2021). They allow users to control their self-presentation content and, at same time, elevate sharing information risk (Vgena et al., 2022; Yokoyama et al., 2024). Consequently, choices of disclosure are hardly spontaneous, but are instead result of an ongoing appraisal of expected rewards and potential harms. This decision-making process can be most characterized according to Privacy Calculus Theory (PCT), which posits that individuals balance perceived benefits against perceived costs before deciding whether or not to

disclose personal data (Dienlin and Metzker, 2016; Ostendorf et al., 2022).

However, risk has been disproportionately understudied in existing literature as a generalised construct (like privacy concern) (Cheung et al., 2015; Dienlin and Trepte, 2015). This asymmetry limits our understanding of disclosure behavior, in particular, in culturally specific situations when risks are not merely technological, but also experiential and contextual. Self-disclosure in collectivist cultures, such as Pakistan, is hidden beneath social norms, and concers regarding privancy and social judgment. In a similar fashion, whereas problem of privacy is widely researched, privacy invasion experience role, which is actual exposure to misuse of personal information, harassment, or data breach, has been under-researched (Gonsalves et al., 2023; Memarian et al., 2025). In contradiction of abstract issues, lived experiences of privacy violation may have a significant impact on risk perceptions, trust, and vulnerability of users, thus affecting their willingness of sharing data online (Ali, 2025; Younis et al., 2025).

Notably, digital risks do not passively affect users. With privacy settings, selective sharing, and boundary regulation strategies, people actively cope with disclosure of their information. This feature, which can be conceptualized as privacy control, reflects how users perceive ability to regulate access to their personal information and have control over their online identity (Darwish & Ghazinour, 2019; Loh et al., 2024). Based on Communication PCT, privacy control is a key factor that influences disclosure decisions by balancing the connection between perceived risks and actual behaviour (Rodríguez-Priego et al., 2023).

While there is an increasing use of the Internet and social media in Pakistan, and self-disclosure research is moving forward in this area, there is limited and fragmented empirical research on self-disclosure online in Pakistan (Maqsood & Ashfaq, 2022; Nabeel & Iqbal, 2025). Existing studies have mainly included general privacy concerns and perceived risks and largely forgotten privacy invasion experience as a unique experiential risk factor (Cheung et al., 2015; Dienlin & Trepte, 2015; Memorian et al., 2025). Moreover, there is limited evidence from previous research on the ability of privacy control to diminish or modify the impact of privacy-related experiences on disclosure behaviour (Darwish & Ghazinour, 2019; Loh et al., 2024; Rodríguez-Priego et al., 2023).

The lack of awareness of the actual experiences of privacy invasion and how they influence online self-disclosure, as well as whether privacy control is a protective mechanism among social media users in Pakistan, has not yet been studied (Gonsalves et al., 2023; Ali, 2025; Younis et al., 2025). This gap is significant since disclosure in Pakistan is likely to be affected by cultural factors such as privacy, reputation, and social judgement that do not necessarily correlate with the same factors in the West. Therefore, this study investigates relationship between privacy invasion experience and online self-disclosure among Pakistani university students and examines whether privacy control moderates this relationship.

Research Objectives

RO1: To analyze privacy invasion experience impact on online self-disclosure.

RO2: To investigate the moderating role of privacy control in the relationship between privacy invasion experience and online self-disclosure.

Research Questions

RQ1: What is privacy invasion experience impact on online self-disclosure?

RQ2: Does privacy control moderate the relationship between privacy invasion experience and online self-disclosure?

Literature Review and Hypotheses Development

Online Self-Disclosure and Privacy Calculus

Online self-disclosure is voluntary sharing of personal information over Internet, and it spans a wide spectrum of information that includes shallow details about oneself as well as deep-seated personal beliefs and experiences (Bazarova and Choi, 2014; Davis, 2012). Disclosure form in discursive environment of social networking platforms is conditioned by platform affordances (persistence, visibility and diversity in audience)

that precondition disclosure in offline context of interpersonal communication (Hollenbaugh, 2021). Even though disclosure is beneficial to build relationships and participate in social interactions, it also exposes people to numerous risks, which is a complex and context-dependent behavior (Vgena et al., 2022; Yokoyama et al., 2024).

PCT offers a hegemonic explanatory mode of comprehending this complication. It assumes that people make a cost-benefit analysis during which they think about advantages they may receive by sharing personal information and risks they may face in process (Laufer and Wolfe, 1977; Dienlin and Metzker, 2016). Disclosure occurs when perceived benefits outweigh perceived costs, and disclosure increases with increased risk perception (Cheung et al., 2015). However, even these measures cannot be deemed as completely rational; they are affected by society norms, past experiences and cultural backgrounds and, therefore, not entirely consistent when it comes to disclosure behavior within different societies (Baruh et al., 2017; Ostendorf et al., 2022).

Privacy Invasion Experience and Self-Disclosure

While privacy concerns have been studied, role of privacy invasion experience has not widely studied. Although problems of privacy have already been extensively researched, contribution of experience of privacy invasion brings about a more tangible and behaviorally meaningful dimension of perceived risk. Privacy invasion is a concept that describes actual cases of having become a victim of an invasion of personal information that was accessed, abused, or exposed without your consent (such experiences as data breach, cyber harassment, identity abuse, or unauthorized sharing of content).

In terms of privacy calculus, these experiences result in a larger salience of perceived risk, in that they directly indicate that one may be harmed. In contrast to abstract issues, lived experiences of privacy violation can redefine trust level that users have in digital platforms, increase perceived vulnerability and also encourage more cautious or restrictive disclosure behaviors (Ali, 2025; Younis et al., 2025). Such experiences can also cause defensive communication strategies, including minimizing audience visibility, minimizing content sharing or not discussing sensitive topics altogether.

Another theory that substantiates this argument is Communication Privacy Management Theory (CPMT), suggesting that people respond to turbulence or boundary crossing by adjusting boundaries of their privacy (Petronio, 2002). Negative experiences disrupt privacy rules, which lead to boundary reinforcement, thus diminishing tendency to be more open and particular to disclose. In that respect, invasion experience of privacy not only amplifies perceived cost but also changes underlying mechanisms that are involved in management of privacy.

H1: Privacy invasion experience negatively influences online self-disclosure.

Moderating Role of Privacy Control

Although perceived risks play a critical role in shaping disclosure behavior, individuals differ. Even though perceived risks are of critical importance in determining disclosure behavior, people have varying capacities to handle perceived risks. Concept of privacy control describes how users feel about their perceived ability to control access to their personal information using tools as privacy settings, audience segmentation, and selective disclosure strategies (Darwish and Ghazinour, 2019; Loh et al., 2024).

In terms of CPMT, privacy control concept is conceptualized as a process by which people create and sustain boundaries around their personal information. Increased perceived control allows users to feel more confident in controlling their digital identity, thus minimizing effects of perceived risks on disclosure decision-making. On the other hand, with a perceived lack of control over their information, even moderate threats can have a big deterrent effect on disclosure.

Considering privacy calculus as concept of privacy control, one can consider that privacy control is concept that changes process of cost-benefit evaluation. Privacy control can reduce adverse correlation between perceived risk and self-disclosure by increasing confidence level of users in their capacity to reduce risks. This

implies that users who have a higher control level are more likely to persist in disclosing information despite existence of risks, as compared to users with a lower control level.

H2: Privacy control moderates the relationship between privacy invasion experience and online self-disclosure, such that the negative effect is weaker at higher levels of privacy control.

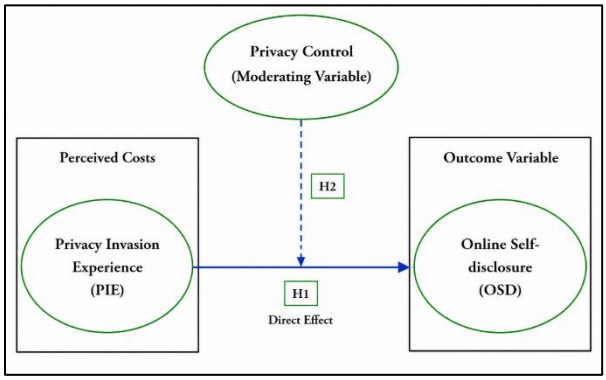

Figure 1: ***Conceptual Framework***

Methodology

Research used quantitative, cross-sectional research design to address issue of relationships between perceived risks and online self-disclosure, as well as moderating role of privacy control among university students in Pakistan. A survey-based research design was used because it was an ideal research design to test theoretical grounded models and evaluate latent constructs of attitudes, perceptions, and behavioral intentions (Hair et al., 2017). Target population was comprised of students pursuing their degree programs through both public and private universities of major provinces in Pakistan and represented a digitally active segment of population with a higher engagement level in social networking sites.

A structured questionnaire based on a previous version of developed scales was used to gather data that were valid and respondent-friendly in terms of measurement and conceptualization. Tool comprised online self-disclosure, experience of invasion of privacy, and experience of control in terms of privacy. Items were operationalized with a five-point Likert scale between SD and SA, and measurement consistency of respondents' perceptions and behaviors was ensured. Pre-testing of questionnaire was done to ensure that it was clear, reliable and contextually relevant before actual data collection. Operational definitions of study variables were adapted from established literature to ensure conceptual clarity and measurement validity, as presented in Table 1.

Table 1.

Operational Definitions of Variables

Variable	Definition	References
Online Self-Disclosure	Personal information voluntary sharing, thoughts, feelings, experiences, and opinions through online platforms and social networking sites.	(Bazarova & Choi, 2014; Davis, 2012)
Privacy Invasion Experience	Individuals' prior experiences involving unauthorized access, misuse, exposure, or violation of personal information, including cyber harassment, data breaches, and privacy-related incidents in online environments.	(Ali, 2025; Memarian et al., 2025)
Privacy Control	Perceived ability of individuals to regulate access to their personal information, manage privacy settings, and control disclosure boundaries in digital environments.	(Darwish & Ghazinour, 2019; Petronio, 2002)

There were 443 valid responses obtained using non-probability sampling methods, which was consistent with similar studies carried out in digital communication research where access to respondents was mediated through online platforms (Kasmani et al., 2022; Towner et al., 2022). Sample size met suggested cutoffs of structural equation modelling, as well as offered adequate statistical strength to test hypotheses. Respondents were of different demographic backgrounds as regards gender, age and geographical distribution, which increased

findings generalizability to population in university.

Data analysis was carried out with SmartPLS software using PLS-SEM. This method was suitable for predictive research models that imply multiple constructs and moderating effects, especially when aim of research was extension of theory but not its confirmation (Hair et al., 2017). Analysis was done in two steps: first, assessed measurement model to test reliability and validity of model, and then structural model was analyzed to test relationship between variables that were theorized to occur. Cronbach's alpha and composite reliability were used to assess reliability, whereas convergent validity was analyzed by AVE. Fornell-Larcker criterion and analysis of cross-loading were used to determine discriminant validity.

Evaluations of structural model were path coefficients, coefficient of determination (R^2), effect sizes (f^2) and predictive relevance (Q^2). Interaction terms were used to test moderation effects of online self-disclosure on strength of relationships between perceived risks and online self-disclosure. Multiple resamples bootstrapping procedures were used to establish statistical significance of each path of model, which ensured robust and reliable results.

Altogether, methodological approach was in line with previous research on topic of online self-disclosure and offered a rigorous framework with which interaction between perceived risk, privacy control and digital communication behavior was examined in a culturally specific environment.

Results

Table 2
Demographic Profile (N = 443)

Variable	Category	Frequency	Percentage
Gender	Male	268	60.5%
	Female	174	39.3%
	Prefer not to say	1	0.2%
Marital Status	Single	323	72.9%
	Married	115	26.0%
	Prefer not to say	5	1.1%
Age Group	18–25	289	65.2%
	26–35	104	23.5%
	36–45	50	11.3%
Education Level	Undergraduate	222	50.1%
	Graduate	117	26.4%
	Postgraduate	103	23.3%
Religion	Muslim	418	94.4%
	Hindu	13	2.9%
	Christian	10	2.3%
	Sikh	2	0.5%
Province	Punjab	167	37.7%
	Sindh	111	25.1%
	KPK	80	18.1%

Variable	Category	Frequency	Percentage
	Baluchistan	42	9.5%
	AJK	24	5.4%
	Gilgit-Baltistan	11	2.5%
	Islamabad	8	1.8%
Employment Status	Unemployed	230	51.9%
	Employed	177	40.0%
	Self-employed	36	8.1%

Results indicate that sample is largely composed of young (18–25), single students, with representation across provinces and educational levels. This demographic composition is appropriate for examining online self-disclosure behavior among digitally active youth in Pakistan.

Table 3
Descriptive Statistics of Constructs

Construct	Mean	Std. Deviation
Online Self-Disclosure (OSD)	3.87	0.74
Privacy Invasion Experience (PIE)	3.58	0.77
Privacy Control (PC)	3.92	0.72

Mean values suggest moderate to high levels of self-disclosure and perceived risks among respondents, indicating active engagement with digital platforms alongside awareness of associated threats.

Table 4.
Reliability and Validity

Construct	Cronbach's Alpha	CR	AVE
OSD	0.905	0.930	0.726
PIE	0.882	0.910	0.630
PC	0.939	0.954	0.804

Discriminant validity was verified using HTMT ratios, all of which were below 0.90, and Fornell–Larcker criteria, where diagonal AVE values exceeded inter-construct correlations. Multicollinearity was not a concern, as all VIF values were below 5.

Table 5
Direct Effects

Hypothesis	Path	β	t-value	p-value	Result
H1	PIE → OSD	0.209	3.224	0.001	Supported

Privacy Invasion Experience (β = 0.209) suggests that experiential risks may be influential in shaping disclosure behavior.

Table 6
Moderation Effects

Hypothesis	Path	β	t-value	p-value	Result
H2	PC × PIE → OSD	0.07	1.45	0.14	Not Supported

Findings indicate that privacy control does not significantly moderate relationships between perceived risks and online self-disclosure. This suggests that users' perceived ability to control privacy does not mitigate influence of risk factors in this context.

Table 7
Effect Size

Construct	f^2
PIE → OSD	0.062

These values suggest that both risk factors contribute modestly yet significantly to explaining online self-disclosure.

Table 8
Summary of Hypothesis Testing

Hypothesis	Statement	Result
H1	Privacy invasion experience → OSD	Supported
H2	Privacy control moderates PIE → OSD	Not Supported

Discussion

Present study aimed to study impact of privacy invasion experience on online self-disclosure of Pakistani university students and to explore moderating effect of privacy control. Results showed moderate to high disclosure, privacy concern and privacy control, while most respondents were young adults (18-25) who are very active in digital world.

1. Impact of Privacy Invasion Experience on Online Self-Disclosure

Objective of this study was to explore impact of privacy invasion experience on online self-disclosure of Pakistani university students. Results showed a statistically significant relationship between privacy invasion experience and disclosure behavior in online setting ($\beta = 0.209$, $t = 3.224$, $p = 0.001$), suggesting that privacy invasion experience has a significant impact on disclosure behavior on internet. While effect size was small ($f^2 = 0.062$), findings indicated that experiential privacy-related risks make a meaningful contribution to differences in online self-disclosure.

This finding corroborates PCT which states that people consider risks and benefits of privacy disclosure in online contexts prior to disclosing information (Dienlin & Metzger, 2016). Discovery indicates that privacy breach experiences are integrated into users' risk assessment process and in turn shape future disclosure decisions. Memorian et al. (2025) emphasized significance of privacy related experiences to understand online disclosure behaviors, and Baruh et al. (2017) noted that privacy experiences have a significant effect on privacy management practices. Findings align with those of Gonsalves et al. (2023) and Rodríguez-Priego et al. (2023) who found that perceptions of vulnerability and privacy influence self-disclosure decisions. Similarly, Maqsood and Ashfaq (2022), Nabeel and Iqbal (2025), Ali (2025), and Younis et al. (2025) all revealed that privacy concerns, cyber threats, and digital harassment affect online behavior in Pakistan context. Based on CPMT (Petronio, 2002), privacy intrusion experiences can induce privacy boundary turbulence, which forces an individual to re-evaluate disclosure practices. Results thus

contribute to literature on privacy; they make experiential dimension of privacy invasion a key element in study of privacy risk, and they indicate need for increased awareness and measures related to digital safety.

2. Moderating Role of Privacy Control in the Relationship Between Privacy Invasion Experience and Online Self-Disclosure

Second objective of this study was to explore moderation effect of privacy control on relationship between experience of privacy invasion and online self-disclosure of university students in Pakistan. Findings showed no statistically significant interaction effect between experience of privacy invasion and control over privacy ($\beta = 0.07$, $t = 1.45$, $p = 0.14$). Thus, Hypothesis 2 was not supported. Level of perceived privacy control ($M = 3.92$, $SD = 0.72$) was not significantly different, but perceived privacy control did significantly affect influence of privacy invasion experience on online self-disclosure. These findings suggest that privacy control may not be sufficient to mitigate effects of privacy-related experiences on disclosure behavior.

This finding contradicts predictions of PCT and CPMT which imply that higher perceived control over personal information, lower level of privacy concerns and greater likelihood of disclosure (Dienlin & Metzger, 2016; Petronio, 2002). Finding also differs from previous studies that emphasized importance of privacy-control mechanisms in shaping online behavior. For example, Darwish and Ghazinour (2019) noted how privacy-management tools can impact privacy behavior, and Vgena et al. (2022) identified how privacy-protection mechanisms influence social-media users' decisions. Moreover, Rodríguez-Priego et al., (2023) found that an increase in perceived privacy protection leads to increased self-disclosure, while Loh et al., (2024) suggested that perceived control promotes online participation. Present finding, however, aligns with findings of Memarian et al. (2025) who proposed that privacy concerns are likely to remain even when privacy-management tools are present and Baruh et al. (2017) who suggested that privacy concerns are likely to remain despite presence of privacy-management tools. Despite believing they have sufficient control over their privacy, users may still experience concerns about data misuse, cybercrime, surveillance, and unauthorized access. Results indicate that theoretically, privacy control does not appear to consistently moderate between contexts. In practice, they emphasize importance of enhanced trust-building mechanisms, transparency, cybersecurity, and data governance in addition to privacy-control capabilities.

Implications

Research has theoretical and practical significance in sense of meaning and management of notion of online self-disclosure in new digital environment. Theoretically, study is an extension of PCT that integrates culturally-based and experience-based risk factors in proving that decisions of disclosure are not only influenced by generalized privacy issues, but also by privacy-related and experience-based threat. Research is related to need for better contextualization of digital communication studies and question of universalism of Western conceptions. Concurrently, results restrict scope of CPMT, as it is indicated that privatization control might not be an effective way of managing boundaries, especially in a context where privacy issue becomes more salient than technological regulation.

In practice, results suggest need to undertake more holistic digital literacy programs that would transcend technical aspect of online behavior. Universities and other educational institutions should consider integrating training programs to create awareness of threat posed by privacy and best practices when they get involved in self-disclosure over Internet. Policymakers may also want to improve data protection mechanisms and systems because experiential risks are shown to be important factors affecting user attitude.

In addition, social media platforms need to enhance their privacy-friendly policies and policies regarding trust, safety and content moderation to reduce the perceived risk of disclosure. Finally, the paper underscores the importance of creating a safe and welcoming online space where individuals can freely and safely express themselves without fear of being made vulnerable online. Technology and online

safety issues need to be addressed to ensure that digital platforms can be a place of engagement and not vulnerability.

Limitations and Future Research

There are several limitations of this study. First, cross-sectional design limits causal inferences since relationships are only studied at a specific time. Second, the sample size and use of non-probability sampling and a sample of students limit the generalisability to the population of universities. Third, use of self-reported data can bring in respondent bias.

Future studies can utilise longitudinal or experimental studies to determine causality and analyse variations in disclosure behaviour with time. More generalisability will be gained if the sample is expanded to include a diversity of demographic groups as well as cross-cultural groups. Additionally, other risk scenarios related to context could be explored in future research, and other moderating variables (such as trust or platform type) could be examined to refine the privacy calculus framework further.

Conclusion

The study indicated that experience of privacy invasion can be a significant variable that affects self-disclosure in the online environment among the university students in Pakistan. Experiential risks are likely to be more important than perceived technological control in affecting disclosure behaviour. Results suggest that context is significant when understanding digital behaviour and extends the existing theories with experiential risk dimensions related to privacy.

References

Ali, R. (2025). Silenced online: Women's experiences of digital harassment in Pakistan. Women's Studies International Forum,

Ayub, A., Shehzad, Y., & Ahmad, S. J. Q. J. o. S. S. (2024). Evolution of Communication: A Comparative Study from Cave Paintings to Emojis. *5*(3), 68-74.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017a). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26-53.

Bazarova, N. N., & Choi, Y. H. (2014). Self-Disclosure in Social Media: Extending the Functional Approach to Disclosure Motivations and Characteristics on Social Network Sites. *Journal of Communication, 64*(4), 635-657.

Cheung, C., Lee, Z. W., & Chan, T. K. J. I. R. (2015b). Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence. *25*(2), 279-299.

Darwish, R., & Ghazinour, K. (2019). Photos and Tags: A Method to Evaluate Privacy Behavior. Intelligent Computing-Proceedings of the Computing Conference,

Davis, K. (2012, Dec). Friendship 2.0: adolescents' experiences of belonging and self-disclosure online. *J Adolesc, 35*(6), 1527-1536.

Deuze, M., & McQuail, D. (2020). McQuail's media and mass communication theory. *McQuail's Media and Mass Communication Theory*, 1-688.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383.

Dolan, R., Conduit, J., Frethey-Bentham, C., Fahy, J., & Goodman, S. J. E. j. o. m. (2019). Social media engagement behavior: A framework for engaging customers through social media content. *53*(10), 2213-2243.

Gonsalves, P. P., Nair, R., Roy, M., Pal, S., & Michelson, D. (2023). A systematic review and lived experience synthesis of self-disclosure as an active ingredient in interventions for adolescents and young adults with anxiety and depression. *Administration and Policy in Mental Health and Mental Health Services Research, 50*(3), 488-505.

Hair Jr, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. J. I. J. o. M. D. A. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *1*(2), 107-123.

Hollenbaugh, E. E. H. E. E. (2021). Self-presentation in social media: Review and research opportunities. *Review of communication research*, *9*.

Jones, R. (2013). *Communication in the real world: An introduction to communication studies*. The Saylor Foundation.

Kasmani, M. F., Abdul Aziz, A., & Sawai, R. P. (2022a). Self-disclosure on social media and its influence on the well-being of youth. *Jurnal Komunikasi: Malaysian Journal of Communication, 38*(3), 272-290.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22-42.

Loh, H. S., Martins van Jaarsveld, G., Mesutoglu, C., & Baars, M. (2024). Supporting social interactions to improve MOOC participants' learning outcomes: A literature review. Frontiers in Education,

Malhan, M., Dewani, P. P., Nigam, A., Vaz, D., & Ogbeibu, E. A. A. J. J. o. G. I. M. (2021). Exploring customer engagement on social networking sites: a qualitative research enquiry. *30*(5), 1-28.

Maqsood, M., & Ashfaq, A. (2022). The audience is the key, data is not: analyzing users'concerns and experts'reflections regarding privacy policies of social networking sites. *Pakistan Journal Of Social Research*, *4*(1), 511-520.

Memarian, S., Malgonde, O. S., & Kim, D. J. (2025). Unraveling the Privacy Paradox: A Comprehensive Review of Factors Behind the Discrepancy in Online Concerns and Disclosure Behavior. *Information Systems Frontiers*, 1-22.

Nabeel, F., & Iqbal, K. (2025). Privacy, data protection and cyber crimes: mapping perceptions of Pakistani users. *Journal of Applied Security Research*, *20*(2), 293-319.

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. State University of New York Press.

Rodríguez-Priego, N., Porcu, L., Pena, M. B. P., & Almendros, E. C. (2023). Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure. *Journal of Retailing and Consumer Services*, *72*, 103284.

Schlosser, A. E. (2020, Feb). Self-disclosure versus self-presentation on social media. *Curr Opin Psychol*, *31*, 1-6.

Vgena, K., Kitsiou, A., Kalloniatis, C., & Gritzalis, S. J. F. I. (2022). Determining the Role of Social Identity Attributes to the Protection of Users' Privacy in Social Media. *14*(9), 249.

Yokoyama, K., Ihira, H., Matsuzaki-Kihara, Y., Mizumoto, A., Tashiro, H., Shimada, K., Yama, K., Miyajima, R., Sasaki, T., & Kozuka, N. J. G. (2024). Development of the Self-Assessment Self-Disclosure Questionnaire to Examine the Association between Self-Disclosure and Frailty among Community-Dwelling Older Adults in Japan. *9*(3), 67.

Younis, R., Khan, K. A., Tahir, M. D., Saleem, S., Samad, U., & Nadeem, N. (2025). Socio-Psychological Impact Of Cyber Harassment On Working Women: A Study Of Khanewal District, Pakistan. *Contemporary Journal of Social Science Review*, *3*(3), 1804-1815.