Security Concerns and Behavioural Responses to Social Media Usage among Generation Z: An Empirical Study

Chandrashekhar Ingle[1*], Dr K.Sita Nirmala Kumaraswamy[2]

[1*]Research Scholar, Savitribai Phule Pune University, Pincode: 411007, email: shekhar.ingle@gmail.com, Orcid Id: 0009-0001-4217-1401
[2]Director, D. Y. Patil Institute of Master of Computer Applications and Management, Akurdi, Pune, PIN Code: 411035, email: director@dypimca.ac.in, Orcid Id: 0000-0003-3615-5138

Abstract
Social media has become an integral part of the everyday life of Generation Z, facilitating communication, entertainment, education, networking, and self-expression. At the same time, increased engagement with social media platforms exposes users to concerns relating to privacy, personal data misuse, identity theft, unauthorised access, cyber threats, and other forms of digital risk. The present study examines the behavioural and perceptual determinants of social media security concerns among Generation Z users in an Indian urban context. Specifically, the study investigates the role of social media usage intensity, security awareness, security-related behavioural practices, and perceived control in shaping users' security concerns. The study is based on primary survey data collected from 243 target population and proposes the use of reliability analysis, correlation analysis, regression analysis, and factor analysis to examine the relationships among the selected constructs. The conceptual premise of the study is consistent with previous research demonstrating that privacy and security concerns are associated with users' awareness, perceived control, risk perception, and precautionary behaviour. The uploaded study specifically reports that higher social media usage is associated with greater security concern, whereas awareness, security behaviour, and perceived control are important factors in users' responses to perceived risk. The study contributes to the growing literature on digital security behaviour by integrating behavioural and perceptual dimensions within the specific context of Generation Z. The findings are expected to provide useful implications for educational institutions, social media platform providers, cybersecurity practitioners, and policymakers in designing interventions that promote safer and more responsible social media behaviour.

Keywords: Generation Z; Social Media Security; Privacy Risk; Security Awareness; Perceived Control; Behavioural Practices; Cybersecurity.

1. Introduction

Digital technologies have rapidly changed how people communicate, connect, engage, build identity and conduct social and economic life. Social media has become part of everyday life and offers people the chance to make social connections, share views, share information, get entertainment, join communities and interact with organisations and brands. Mobile, social media platforms like Instagram, Facebook, YouTube, WhatsApp, X, Snapchat, LinkedIn, and new, short video and content sharing apps have increasingly made private/social, educational, professional, and commercial communication indistinguishable. Consequently, social media is no longer just a communication technology, but rather an important part of people's digital identity and daily habits (Ellison et al., 2007; Kaplan & Haenlein, 2010; Kietzmann et al., 2011; Boyd & Ellison, 2007; Appel et al., 2020).

The growing omnipresence of social media in everyday life has sparked a great deal of academic research to comprehend the use, in terms of frequency, and the intensity, of social media. Ellison et al. (2007) developed a new term that combines levels of use and degree of psychological involvement in daily life. Further research has confirmed that the use of social media can impact social capital, self-presentation, interpersonal relationships, well-being, information sharing, and disclosure online (Steinfield et al., 2008; Pempek et al., 2009; Ross et al., 2009; Christofides et al., 2012; Kuss & Griffiths, 2017). Therefore, a knowledge of the Social Media Usage Intensity (SMUI) is important to consider when studying individuals' exposure to privacy and information-security risks.

The more personal information that is being shared through social media has also raised new issues concerning privacy, information security, surveillance, identity protection, and digital safety. Users regularly share photos, personal perspectives, location data, educational and professional information, relationship information, preferences, purchasing habits and other types of personally identifiable or inferential information. This means that users can be subjected to several risks, such as unauthorized collection of personal data, identity theft, phishing, account takeover, cyberstalking, impersonation, social engineering, profiling, and unwanted disclosure of personal data (Krasnova et al., 2009; Krasnova et al.,

2010; Kokolakis, 2017; Baruh et al., 2017).

The issue is even more complicated by the privacy paradox, where people are highly concerned with their privacy yet provide a lot of personal information at the same time and interact with social media platforms on a great deal. Rather, users often trade privacy and security concerns with perceived benefits like social connection, entertainment, convenience, self-expression, and personalization (Krasnova et al., 2010; Kokolakis, 2017; Baruh et al., 2017; Dienlin & Metzger, 2016). Knowing how social media is used, therefore, must take into account not only how much social media is used, but also how socially media is perceived, how much it feels like it has over the user, the risks it poses, and the behavioral reactions.

Human behaviour plays a greater and greater role in information security. Users are also a critical part of the security ecosystem, as they can activate technological security measures like encryption, authentication, firewalls, access control and artificial intelligence threat detection capabilities. Bulgurcu et al. (2010) have shown the importance of General Information Security Awareness (GISA) by proving that the users' beliefs, attitudes and intentions toward the compliance of security policies are influenced by the information-security awareness. Subsequent studies have similarly highlighted the importance of security knowledge, awareness, self-efficacy, and individual capabilities in determining cybersecurity-related behaviour (McCormac et al., 2017; Parsons et al., 2017; Makhdoom et al., 2018). In the context of social media, the importance of information-security awareness is accentuated as great part of threats relies on the users' knowledge of the suspicious behaviour besides only technological protection.

Social media privacy and security perceptions are ultimately manifested in users' behaviours. These can be anything from adjusting privacy settings and disclosure of personal information, to blocking and/or reporting suspicious accounts, avoiding unfamiliar links, making authentication more robust, declining unnecessary permissions, deleting posts, limiting use of the platform, or engaging in other privacy- and security-protective behaviors.

Based on Protection Motivation Theory (PMT), Boerman et al (2021) found that the four elements of perceived severity, perceived susceptibility, response efficacy and self-efficacy are factors that affect online privacy-protection behaviour. Their results suggest that Internet users are not automatically motivated to act in ways to protect their privacy when they know that threats to privacy exist online. Instead, behavioural reactions are based on the threat appraisal and coping ability of the individual. This view offers a theoretical basis for understanding how GISA, security-threat concerns and privacy concerns might come to influence behaviour in the end.

A new study indicates that Generation Z is highly digitally engaged, yet holds complicated views on privacy. Social connection, fear of missing out, social anxiety, personalisation, convenience and perceived benefits all are possible factors to influence their willingness to share information, whilst their privacy-protection behaviour is influenced by privacy concerns, self-efficacy, subjective norms and perceived benefits (Lyngdoh et al., 2023; McKee et al., 2024; Stone & Eveleth, 2026). The fact that Generation Z uses social media to a great extent while also growing up in an era when privacy concerns are more prevalent than ever makes this group a useful population to study the relationship between the intensity of social-media use, awareness of information security, perceptions of privacy/security, and behavioural responses. Limited research has, however, combined Social Media Usage Intensity, General Information Security Awareness, Perceived Control, Social Media Privacy Concerns, Security Threat Concerns and Behavioural Responses in the same explanatory framework.

1.1 Purpose of the Study

This study aims at developing and testing an integrated model that explains behavioural responses to social-media usage among the Generation Z, by examining the influence of SMU intensity and general information security awareness on their behavioural responses, and by examining the role of mediators as Perceived Control, Social Media Privacy Concerns and Security Threat Concerns.

The study is expected to make a significant contribution to the literature by combining the social-media intensity, information-security awareness, privacy calculus, perceived control, security-threat perception and protection motivation factors. The results can also help universities and organizations to develop more specific digital-literacy, privacy-awareness, and cybersecurity measures for Generation Z.

2. Review of Literature

2.1 Social Media Consequences Intensity

Social networking sites have become a popular way to communicate, and have evolved into an integrated part of social, academic, business, and consumer life. Their research found that Facebook intensity was a better predictor of social capital than Internet use and showed the value of looking at how much a platform is part of someone's life, not how much they are using. The Facebook Intensity Scale has been used and/or adapted in subsequent studies to measure social connectedness, psychological outcomes, identity, well-being, and patterns of online engagement (Ellison et al., 2007; Steinfield et al., 2008; Pempek et al., 2009; Ross et al., 2009; Jenkins-Guarnieri et al., 2013; Kircaburun et al., 2018). The scale has therefore become a common means of operationalising social-network intensity, while more recent researchers have suggested the need to take into account a broader range of social media platforms, distinctions between active and passive use of social media, and qualitative differences in intensity of engagement.

The significance of SMUI for privacy and information-

security research is due to the increased amount of information, its frequency, persistence and context diversity, produced by high intensity users of information. Previous social-network studies had already proved that social media offers relational and psychological advantages, which can inspire self-presentation and information disclosure (Ellison et al., 2007; Krasnova et al., 2009; Krasnova et al., 2010; Christofides et al., 2012; Dienlin & Metzger, 2016; Jozani et al., 2020). Importantly, such heavy usage does not automatically mean careless usage: frequent users can gain more familiarity with the platforms at the same time that they become more adept at managing their privacy. This presents an important theoretical dilemma of more exposure to privacy risks versus more experience with privacy controls. For instance, Jozani et al. (2020) found that perceived risk and control can affect social privacy concerns, and these social privacy concerns can affect engagement

When studying behavioural responses relating to privacy and security, this dual possibility becomes pertinent. If a user is exposed and interacting with more information, he or she could be a target of more phishing attempts, malicious links, impersonation, unwanted data collection, targeted advertising, social engineering and inappropriate information requests. Meanwhile, the frequent users might grow more familiar with privacy settings and risks on platforms. Studies have demonstrated that social benefits, fun, maintaining the network, and how the disclosure will be perceived positively can positively motivate disclosure even when there is an awareness of potential risks (Krasnova et al., 2009; Krasnova et al., 2010; Christofides et al., 2012; Dienlin & Metzger, 2016; Baruh et al., 2017; Jozani et al., 2020). This aligns with what's been called the “privacy paradox” when people say they are very concerned about privacy and then they still disclose something or interact heavily with social platforms. Baruh et al. (2017) conducted a meta-analytical study of 166 studies across various topics of SNS privacy concerns, and concluded that privacy concerns generally suppress information sharing and encourage privacy-protective behaviors, but do not necessarily suppress SNS use. Therefore, SMUI is a significant antecedent, and it could be hypothesized that it does act as an influence, but indirectly via users' sense of control, concerns of privacy and security threats.

2.2. General Information Security Awareness

General Information Security Awareness (GISA) is capturing the individual's knowledge and awareness of information-security risks and appropriate practices. A foundational contribution was made by Bulgurcu, Cavusoglu and Benbasat (2010) who found that information security awareness had an impact on employees' beliefs and attitudes about compliance with information-security policies. In their empirical study, they measured security awareness with an index that included 464 respondents, finding that security awareness had a positive impact on outcome beliefs and attitudes, which in turn had a positive impact on compliance intentions. The study is significant because it shifted the focus of information-security research from a purely technological into a user-centric perspective, making user awareness a crucial part of an organisation's information security (Bulgurcu et al., 2010). Other research also shows that security awareness, knowledge, self-efficacy, digital literacy and experience affect users' ability to identify and react to online risks (McCormac et al., 2017; Parsons et al., 2017; Makhdoom et al., 2018; Boerman et al., 2021; Chung et al., 2021; Stone & Eveleth, 2026). The impact of GISA is further enhanced in social media contexts as many security attacks take advantage of the human component and not solely the technical one. Research in mobile security awareness shows that users have different levels of awareness and that mobile environments are unique due to the amount of personal information held on the smartphone, and the constant connectivity between the smartphone and the user (Makhdoom et al., 2018; Alharbi et al., 2020). Research on privacy-protective behaviour also indicates that awareness, Internet skills, technical knowledge and experience have positive relationships with privacy-protective behaviour (Baruh et al., 2017; Büchi et al., 2017; Chanchary et al., 2018; Ham, 2017; Park, 2013; Boerman et al., 2021). Accordingly, awareness is not simply a cognitive tool, but may have an impact on threat perceptions, including their threat intensity and perception of threat probability, as well as whether protective action is justified.

But knowing about something does not necessarily lead to safe behaviour. According to Protection Motivation Theory, people can react to threats in terms of threat appraisal and coping appraisal. To be effectual, users should feel the threat is threatening enough and personally relevant to them, and that they have the ability and means to respond to it (Rogers, 1975; Witte, 1992; Boerman et al., 2021). A person can thus become aware of how information from social media can be misused, but still engage in risky behaviors if the perceived benefits of these behaviors (convenience, social) outweigh the perceived costs, or if the person feels that protective measures are not working for them. This distinction also offers a conceptual linkage between the two types of mediators that are proposed in this study, namely, security awareness may lead to perceived threat, which in turn may lead to behavioural responses, but perceived control and privacy concerns may influence the translation of security awareness to behavioural responses. Research that connects security awareness, perceived control, privacy concerns, risk perceptions, and protective behaviour (Bulgurcu et al., 2010; Baruh et al., 2017; Jozani et al., 2020; Chung et al., 2021; Muhammad et al., 2024; Stone & Eveleth, 2026) supports this integrated interpretation.

2.3 Perceived Control

Perceived control is the degree to which people feel

they have a say over the information they deem relevant to be shared, with whom, when, and how it will be used. This construct is becoming central to privacy-calculus research not only because it considers the potential benefits and risks of the information flow, but also because it considers the ability of the users to control the flow of information. Krasnova et al. (2010) showed that privacy concerns can cause withholding of disclosure, while trust and perceived control options can reduce perceived privacy concerns. Theoretically, this finding is important because it points to how privacy decisions are not just made based on concern but also on whether the person thinks there are enough mechanisms in the environment to control their privacy (Krasnova et al., 2009; Krasnova et al., 2010; Dienlin & Metzger, 2016; Baruh et al., 2017; Jozani et al., 2020; Chung et al., 2021).

Perceived control could thus serve as a psychological linkage between social-media use and behavior. Highly active users might get to know privacy settings, blocking, audience controls, reporting and account-security procedures. There is strong support for this argument in the recent evidence from a meta-analysis, perceived control is positively correlated with social-network-site use, disclosure, and privacy protection. The conclusions indicate that control is not only a deterrent to social-media use, but it can also serve as a facilitator for engagement and protection: When users feel empowered to control information, they may also feel comfortable using social media and simultaneously manage their privacy boundaries.

Krasnova et al. (2009) discovered that the level of information disclosed decreased with organisational privacy concerns, while social concerns brought about greater conscious control over disclosure. Meanwhile, Jozani et al. (2020) showed that perceived control had a negative effect on social privacy concerns and Chung et al. (2021) illustrated the significance of information-security awareness and perceived privacy control on privacy management. Hence, perceived control is a plausible mediator between the awareness and usage experiences and the privacy-related behavioural responses, and is therefore a suitable construct to explain this relationship. Thus, it makes sense to conceptualise perceived control as a mediating variable between awareness and usage experiences with privacy-related behavioural responses.

2.4 Social Media Privacy Concerns

Social Media Privacy Concerns are the apprehensions of people about the collection, use, disclosure, visibility and possible misuse of personal data in social-networking settings. Krasnova et al. (2009) laid one of the important foundations for this by dividing privacy concerns in online social networks into two components, namely organisational and social threats. In their empirical study with 210 participants, they showed that privacy concerns have behavioural effects, with organizational threats leading to decreasing disclosure of information, and social threats to increasing conscious control over information disclosure. These differences between institutional and social privacy concerns have since been supported by studies indicating that there are two types of privacy concerns, relating to organisational information practices and interpersonal contexts (Krasnova et al., 2009; Krasnova et al., 2010; Christofides et al., 2012; Jozani et al., 2020; Baruh et al., 2017; Muhammad et al., 2024).

There is, however, a complex relationship between privacy concerns and behaviour. Meta-analysis shows that privacy concerns are negatively related to disclosure intentions and positively to privacy-protective behaviours, and the correlation between privacy concerns and actual social network use varies from a weak negative relationship to a weak positive one (Baruh et al., 2017; Kokolakis, 2017; Zhu et al., 2021; Jozani et al., 2020). The same size of study, which included 181 studies and about 99,000 observations, revealed that perceived risk, trust and behavioural consequences are all correlated with privacy concern, with the relationships between these variables depending on context and moderator (Xu et al., 2023). These results support the notion that privacy concern should not be viewed as a straightforward determinant of social media usage.

This is especially true for heavy users of social media. Increased involvement means more opportunities for disclosure, surveillance, data collection, social comparison, unwanted contact, and exposure to privacy violations. However, the same heavy users might feel more comfortable with platform functions, and more positive about the advantages of ongoing use. Jozani et al. (2020) determined that social privacy concerns as well as institutional privacy concerns can hinder engagement; but that perceived control and perceived risk have different effects on privacy concerns. Evidence that is more recent among Instagram users also shows that privacy concerns can exist alongside their continued use of social media and may manifest through other mechanisms like trust, fatigue, and privacy-protection behaviour (e.g., recent work on Instagram). Hence, privacy literature has been growing increasingly to favor a privacy-calculus view, viewing privacy as weighed by perceived benefits, risks, control, and behavioral costs rather than by a yes/no response.

2.5 Security Threat Concerns

There is no simple correspondence between privacy concerns and security concerns. Security threat concerns primarily are more directly related to the ability of information, accounts, systems or transactions to be compromised or breached by threats including access, identity theft, impersonation, fraud, phishing, confidentiality violation, integrity violation, and authentication failure; privacy concerns are more related to the ability for the information to be collected, used, disclosed, or made visible

inappropriately. Bansal (2016) explicitly challenged the difference between privacy and security concerns and created the Internet Users Information Transmission Security Concern scale that has two dimensions – authentication and confidentiality, integrity and non-repudiation. The conceptual difference is relevant for social-media studies because a user might feel comfortable with allowing the collection of data on the platform but at the same time be concerned with the risk of hacking or identity theft; or concerned about privacy but not aware of the technical threats.

Concern about security threats can impact behavioral reactions because it is a part of protection motivation. Based on the Protection Motivation Theory (PMT) by Boerman et al. (2021), the study found that the perceived severity and perceived susceptibility of online privacy threats were significant factors in privacy-protective behaviour, as were self-efficacy and response efficacy. Past research on cybersecurity has revealed that awareness and perceived vulnerability can influence users' willingness to use security measures, and past research on mobile security has shown that users' levels of cybersecurity awareness are significantly different and that human vulnerabilities are a key avenue for social engineering attacks (Bulgurcu et al., 2010; Parsons et al., 2017; Makhdoom et al., 2018; Boerman et al., 2021; Muhammad et al., 2024; Stone & Eveleth, 2026). GISA can therefore be related to increased security threat concerns as security threat concerns may lead to increased protective behavioral responses, and the knowledgeable user could be better able to recognize potential threats.

The difference between privacy and security issues is particularly relevant in the current social media landscape due to the existence of different and overlapping risks faced by users. Recent research on social media users with respect to privacy and security concerns shows that privacy and security concerns can be differentiated into distinct groups based on their attitudes towards digital footprints and their adaptation behaviours, further emphasizing the need to consider privacy and security concerns as related yet distinct constructs (Muhammad et al., 2024). Adding SMC to STC thus gives a broader understanding of behavioural responses than the use of only the privacy concern.

The ultimate merit of SMUI, information-security awareness, control, privacy concerns, and security concerns is that they provide the ability to account for what users actually do in reaction to the opportunities and threats of social media. Behaviours may involve restricting sharing of information, adjusting privacy controls, blocking or reporting suspicious accounts, deleting posts or personal information, increasing the strength of authentication, avoiding suspicious links, limiting platform interactions, refusing permissions, using privacy-enhancing tools, or continuing to interact with the platform while limiting the sharing of information. Protection Motivation Theory is a particularly useful theory for providing a theoretical basis (Boerman et al., 2021). In their two-wave study, with 928 respondents, they found that privacy-protective behaviours were not happening consistently, although respondents reported high levels of perceived threats to online privacy. Importantly, perceived severity and response efficacy were correlated with protective behaviour; that is, threat perception needs to be coupled with beliefs about coping response effectiveness.

This multi-dimensional interpretation of behaviour responses is supported by the wider literature. Generally, privacy concerns will lead to protective action, but not necessarily to the abandonment of social media. Baruh et al. (2017) confirm this finding by reporting that there is a link between privacy concerns and using privacy-protective measures. Kokolakis (2017) suggests that even though privacy paradox has been shown to be a relevant explanation for discrepancies between declared privacy attitudes and actual behaviour, it has not been empirically studied by as many other researchers. Chung et al. (2021) also demonstrated that information-security awareness and perceived information-privacy control are pertinent to social-media-related information-privacy management and self-disclosure. Other more recent research classifies users based on their privacy and security orientations and reveals that these orientations have an impact on social-media adaptation (Muhammad et al., 2024). However, behavioural responses must be considered as a continuum from risk-taking and disclosure of information, to selective disclosure, to privacy management, to security protection, to usage reduction, rather than an either/or scenario.

2.6 Need for research in Generation Z

The literature review conducted earlier has shown that the proposed variables are related to one another, but there is a lack of research concerning their relationship among Generation Z social-media users. The young generation is an especially significant one as they are living in the era where social media has become a part of social, educational, professional, entertainment, and consumption experiences. Social and psychological aspects can influence willingness to share personal information, as seen in studies focusing on Gen Z's, including social anxiety, social isolation, fear of missing out, rumination, and perceived privacy care (Lyngdoh et al., 2023). Importantly, this research had been carried out with Gen-Z participants in India, thereby emphasizing the need for studying information sharing and privacy decisions in India instead of making generalizations of the findings from older western samples to Indian digital natives. Other research has also explored the digital privacy calculus of Gen Z, and identified that they are able to balance privacy-protective behaviors like using privacy-enhancing technologies (PETs) and ad blocking with personalisation benefits (McKee et al., 2024).

This is particularly true for recent cybersecurity literature, which has highlighted the need for research for Gen-Z. For instance, Stone and Eveleth (2026) explored privacy protection behavior among Generation Z by analyzing 365 student responses and discovered that privacy concerns, privacy-related self-efficacy, subjective norms, and perceived benefits are related to privacy-protection behavior. The findings indicate that Gen Z's desire to engage with digital innovation can lead to a paradox between the positive aspects of using technology and the privacy/security protection. This is especially applicable to the current study as it suggests that digital natives are not necessarily digitally secure users. Rather, high levels of social media engagement can coexist with limited awareness, sense of lack of control, privacy concerns, and inconsistent engagement in protective behaviours. This combined approach can contribute to understanding how two individuals who are both active in social media may differ in their response to the same risks – one might identify risks, perceive a high level of control, and take protective action; and the other might identify risks, but not feel a sense of control, or feel that the social benefits and convenience outweigh the risks, making them less likely to adopt protective measures. It aligns with the privacy-calculus (Krasnova et al., 2009; Krasnova et al., 2010), protection-motivation (Bulgurcu et al., 2010), and information-security-awareness perspectives (Baruh et al., 2017; Boerman et al., 2021; Muhammad et al., 2024) and addresses the call for studies to investigate the interplay between privacy, security, control, awareness, and actual behaviours (Krasnova et al., 2009; Krasnova et al., 2010; Bulgurcu et al., 2010; Baruh et al., 2017; Boerman et al., 2021; Muhammad et al., 2024).

2.7 Research Gap:

Although significant progress has been made in the literature, there are four significant gaps. First, the previous literature has mainly focused on social-media intensity, privacy concern, information security awareness, or privacy-protective behaviour in isolation without a framework that considers a social-media intensity and privacy concern as integrated factors. Second, privacy concerns and security-threat concerns are often mixed in the same way although they are different types of risk; Bansal's (2016) distinction shows the need to conceptualize security and privacy as interrelated but distinct. Third, perceived control is frequently regarded as the antecedent of disclosure rather than as a mechanism which could account for the relationship between social media engagement and security awareness and behaviors. Fourth, many of the fundamental research studies were done in a pre-smartphone, pre-algorithmic, pre-short video, pre-influencer, pre-AI-driven targeting, pre-digital identity, and pre-sophisticated cyber attack world. These restrictions are especially relevant for the social media habits of Generation Z, as it has a social media usage that is significantly different from the Facebook-based social media environments in which several scales were originally developed.

Thus, the proposed study can meaningfully contribute by investigating the influence of Social Media Usage Intensity and General Information Security Awareness on behavioural responses with the factors of Perceived Control, Social Media Privacy Concerns and Security Threat Concerns for the generation Z. The model combines the behavioural risk factor (SMUI) with the cognitive risk factor (GISA) to both psychological factors, namely control and risk appraisal. Recent evidence has shown that the focus on Gen Z is particularly warranted given that this generation has shown itself to be highly engaged in the digital sphere, has a significant tendency to share information and is also becoming more aware of the need for privacy protection features. Therefore, the study of this integrated model among the Gen-Z users can provide theoretically relevant evidence on transition from social media use to awareness/control and risk perception to a behavioural response and practical implications for universities, employers, the policy makers, and social media platforms in order to bolster responsible digital behaviour among the new generation of digital workers.

2.8 Statement of the Problem

Social media has become a vital part of the lives of the Gen Z. The platforms offer a great deal of means to communicate, entertain, learn, share and express oneself, but they also involve higher usage, which raises privacy concerns, personal data security, unauthorised access, digital footprints and other cyber security issues. Although social media are pervasive among Generation Z, an important question remains: Is increased exposure to social media related to increased security concerns, and how can users' security awareness, security behaviours, and perceived security control impact their reactions to concerns? The literature shows that there are interactions between risk perception, awareness, perceived control and precautionary behaviour, and that the nature of these interactions could vary depending on the context and the population. The source study indicates that among Generation Z users, social media usage intensity, security awareness, behavioural practices and perceived control are considered as the key determinants examined with regard to security concern.

Thus, the main problem of the study is to investigate the association between usage intensity, awareness, behavioral practices, perceived control with the behavioral and perceptual factors affecting social media security concerns among the participants who are users of Generation Z.

2.9 Objectives of the Study

The objectives used for guiding the study are as follows:

- To investigate the relationship between the

intensity of social media use and security concerns of the users of Generation Z.

- To determine the security awareness and security related behaviour among the social media users in generation Z.
- To analyze the effect of perceived control on social media security concerns and social media behavioral responses of Generation Z users.
- To determine the dominant behavioral and perceptual factors that affect social media security concerns of the users from Generation Z.

2.10 Research Hypotheses

In view of the objectives and literature review, the following are the null hypotheses which are to be tested empirically:

H01: There is no significant correlation between intensity of social media use and security concerns regarding social media among Generation Z users.

H02: Security awareness and social media security concerns have no significant relationship for users from generation Z.

H03: Social media security concerns are not significantly related to security-related behavioural practices among members of Generation Z.

H04: There is no significant difference between the perceived control and social media security concern of Generation Z users.

H05: There is no significant interaction between the social media usage intensity, security awareness, behavioural practices and perceived control that influences social media security concerns for Generation Z users.

Research Methodology

3.1 Research Design

It is an explanatory, quantitative and cross sectional study. Primary data will be gathered by conducting a structured questionnaire on Generation Z, who are the users of social media. The study considers the effect between the Social Media Usage Intensity (SMUI) and General Information Security Awareness (GISA) on the Behavioural Responses to Social Media Usage with the Perceived Control, Social Media Privacy Concerns and Security Threat Concerns as the mediating variables.

3.2 Research Approach

The deductive research method is used because the study derives hypotheses from the existing theories and empirical evidence, and then hypotheses are tested with primary data in quantitative research method. The proposed relationships are based on the literature review on social-media usage, information-security awareness, privacy calculus, perceived control and protection motivation.

3.3 Type of Study

The study is an explanatory empirical study to examine the relationship between several latent variables. It is cross-sectional because information will be gathered from respondents at one time. The unit of analysis is the social-media using Generation Z individual.

3.4 Target Population

The target group is Generation Z (social media user) in India. In order to make sure that all participants are adults, Generation Z respondents (age: 18-29 years) are recommended for this study. Respondents must actively use at least one social-media platform and have experience using social media for a minimum of six months.

3.5 Sampling Frame

Since there is no complete national database of Generation Z social-media users, the sampling frame will be built in the following manner: Via: universities, colleges, professional institutions, young professionals, student networks and online communities. Multiple institutions and geographic areas will be used to broaden the diversity of respondents and minimize reliance on a single institutional population.

3.6 Sampling Technique and sampling size

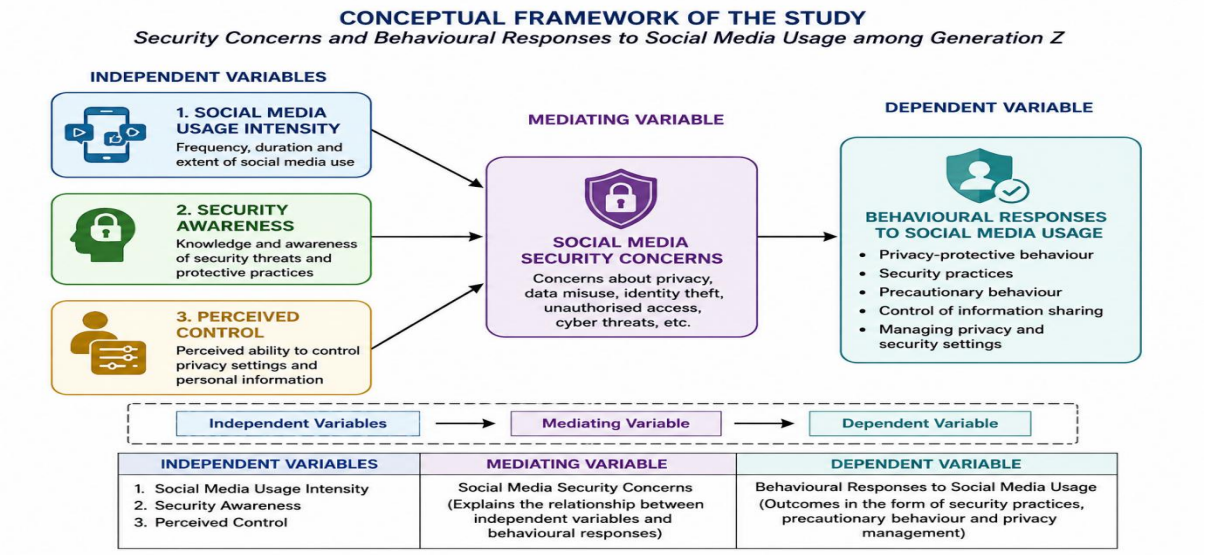
Purposive sampling will be utilized for the study, since the respondents should meet the set criteria among the Generation Z users. A total of 243 usable responses collected to run the PLS-SEM model.

3.7 Data Collection

Structured online questionnaire will be used to gather primary data. The questionnaire will include screening questions, demographic information as well as measurement items for all study constructs. The academic research purpose, voluntary participation, confidentiality and anonymity will be explained to the respondents before they provide informed consent.

3.9 Variables and Measurement

Ellison et al.'s original Facebook Intensity Scale contains both behavioural and attitudinal indicators, while Krasnova et al. (2010) used three items for perceived control. Bansal's (2016) instrument measures information-transmission security concerns through authentication, confidentiality, integrity and non-repudiation dimensions. Boerman et al. (2021) measured online privacy-protective behaviour. These instruments should therefore be adapted rather than represented as newly developed scales.



Source : Authors Work

4. Results

4.1 Assessment of the Measurement Model (Reliability and Validity)

To check the internal consistency reliability, convergent validity, discriminant validity, and composite reliability, the standard criteria of Partial Least Squares Structural Equation Modeling (PLS-SEM) and Confirmatory Factor Analysis (CFA) were used (Hair et al., 2021).

Internal Consistency & Composite Reliability: Cronbach's alpha values were between .835 and .918, which is greater than the accepted value of .70 as shown in Table 1. Likewise, the internal consistency of the latent constructs was high with Composite Reliability (CR) ranging from .888 to .932.

Convergent Validity: All items had an outer loading between .683 and .881, which meets the minimum factor loading criterion of .60. Convergent validity was confirmed as average variance extracted (AVE) ranged from .577 to .753 with 0.50 as the minimum acceptable value (Fornell & Larcker, 1981).

Discriminant Validity: Fornell-Larcker criteria were satisfied (Table 1) with the square root of the AVE for each construct (> .760 to .868) being larger than the highest squared inter-construct correlation.

Table 1: Discriminant Validity & Latent Variable Correlations (Fornell-Larcker Criterion)

Construct	SMUI	SA	PC	PCON	SCON	PSPB
SMUI	0.794					
SA	0.338	0.766				
PC	-0.19	-0.117	0.868			
PCON	0.333	0.446	-0.365	0.814		
SCON	0.31	0.417	-0.368	0.896	0.783	
PSPB	0.262	0.29	-0.204	0.507	0.492	0.76

4.2 Exploratory Factor Analysis (EFA) & Measurement Model Fit

Prior to structural testing, EFA was evaluated for suitability (Table 2). The KMO measure of sampling adequacy was 0.930 ("marvelous" per Kaiser, 1974), and Bartlett's Test of Sphericity was statistically significant (630) = 4,909.35, p < .001).

Table 2: KMO and Bartlett's Test

Statistic / Metric	Value
Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy	0.93
Bartlett's Test of Sphericity — Approx. Chi-Square ($\chi 2$)	4,909.35
Degrees of Freedom (df)	630
Significance (p-value)	<.001

CFA model fit indices (Table 3) confirmed robust fit for the overall measurement structure: $\chi 2/df = 1.842$, CFI = .928, TLI = .919, RMSEA = .059 (90% CI [.052, .066]), and SRMR = .051, satisfying standard thresholds (Hu & Bentler, 1999).

Table 3: Model Fit Indices for Measurement Model

Fit Index Metric	Recommended Threshold	Structural / CFA Model Value	Interpretation
Chi-Square ($\chi 2$) / df	< 3.0	1.842	Excellent fit
Comparative Fit Index (CFI)	> 0.90	0.928	Good fit
Tucker-Lewis Index (TLI)	> 0.90	0.919	Good fit
Root Mean Square Error of Approximation (RMSEA)	< 0.08	0.059	Acceptable fit
Standardized Root Mean Residual (SRMR)	< 0.08	0.051	Good fit

4.3 Structural Model and Hypothesis Testing

Structural paths and direct relationships were evaluated using 5,000 bootstrap resamples (Table 5):

Hypothesis	Path / Relationship	Original Sample (β)	Sample Mean (M)	Std. Error (SE)	t-Statistic	p-Value	Decision
H1	SMUI → PCON	0.161	0.16	0.059	2.715	0.007	Supported
H2	SA → PCON	0.385	0.386	0.061	6.313	<.001	Supported
H3	PC → PCON	-0.28	-0.281	0.052	5.386	<.001	Supported
H4	SMUI → SCON	0.136	0.136	0.057	2.388	0.018	Supported
H5	SA → SCON	0.341	0.342	0.059	5.788	<.001	Supported
H6	PC → SCON	-0.274	-0.274	0.05	5.455	<.001	Supported
H7	PCON → PSPB	0.264	0.265	0.115	2.287	0.023	Supported
H8	SCON → PSPB	0.168	0.169	0.119	1.409	0.16	Not Supported
H9	SMUI → PSPB	0.084	0.084	0.056	1.486	0.138	Not Supported
H10	SA → PSPB	0.054	0.055	0.062	0.865	0.388	Not Supported
H11	PC → PSPB	-0.008	-0.009	0.052	0.163	0.871	Not Supported

Predicting Privacy Concerns (PCON, R^2 = .319): Social Media Usage (β = .161, t = 2.715, p = .007) and Security Awareness (β = .385, t = 6.313, p < .001) significantly increase privacy concerns, whereas Perceived Control exerts a significant negative effect (β = -.280, t = -5.386, p < .001).

Predicting Security Concerns (SCON, R^2 = .294): Social Media Usage (β = .136, t = 2.388, p = .018) and Security Awareness (β = .341, t = 5.788, p < .001) significantly elevate security concerns, while Perceived Control significantly reduces them (β = -.274, t = -5.455, p < .001).

Predicting Behavioral Response (PSPB, R^2 = .276): Privacy Concerns significantly predict behavioral response (β = .264, t = 2.287, p = .023). However, direct paths from SMUI (p = .138), SA (p = .388), and PC (p = .871) to PSPB were not statistically significant in the full structural model, suggesting indirect effects through mediation.

4.4 Mediation Analysis (Indirect Effects):

Mediation was evaluated using non-parametric percentile bootstrapping with 5,000 samples (Preacher & Hayes, 2008).

Table 6: Specific & Total Indirect Effects (Bootstrapping N = 5,000)

Path / Relationship	Indirect Effect (β)	Boot SE	95% CI Lower	95% CI Upper	p-Value	Mediation Type
SMUI → PCON → PSPB	0.042	0.025	0.003	0.101	0.026	Full Mediation
SMUI → SCON → PSPB	0.023	0.019	-0.006	0.068	0.223	No Mediation
SMUI Total Indirect Effect	0.065	0.027	0.017	0.122	0.017	Significant Total Indirect
SA → PCON → PSPB	0.101	0.045	0.016	0.194	0.026	Full Mediation
SA → SCON → PSPB	0.058	0.039	-0.017	0.14	0.143	No Mediation
SA Total Indirect Effect	0.158	0.034	0.096	0.231	<.001	Significant Total Indirect
PC → PCON → PSPB	-0.073	0.034	-0.143	-0.012	0.031	Full Mediation
PC → SCON → PSPB	-0.047	0.033	-0.115	0.012	0.15	No Mediation
PC Total Indirect Effect	-0.12	0.028	-0.18	-0.069	<.001	Significant Total Indirect

Privacy Concerns (PCON) as a Mediator: Privacy Concerns significantly mediated the relationships between all three IVs and Behavioral Response:

- SMUI PCON PSPB: Indirect Effect = .042, Boot SE = .025, 95% CI [.003, .101], p = .026.
- SA PCON PSPB: Indirect Effect = .101, Boot SE = .045, 95% CI [.016, .194], p = .026.
- PC PCON PSPB: Indirect Effect = -.073, Boot SE = .034, 95% CI [-.143, -.012], p = .031.

Because the direct paths were nonsignificant in the presence of PCON, Privacy Concerns acts as a full mediator for all three drivers. Security Concerns (SCON) as a Mediator, the indirect paths through Security Concerns (SCON) were not statistically significant (p > .05), indicating that Privacy Concerns is the primary operational mechanism influencing behavioral response in this framework.

5. Implications

This research has significant implications for organisations looking to gain insight into employee reactions to social media and digital environments. The positive impacts of Social Media Usage Intensity (SMUI) on privacy concerns and security concerns suggest that higher exposure and use of social media can boost their perceptions of security and privacy concerns. Security Awareness also bolsters privacy and security concerns, as it can raise the awareness of employees or users about possible risks in the digital world. On the other hand, Perceived Control mitigates both privacy and security concerns, illustrating the need to empower users with more control over their personal data and digital settings.

The most significant practical implication is that of the mediating effect of Privacy Concerns. The

relationships of SMUI with security awareness, perceived control and behavioural response are significantly mediated by privacy concerns, and security concerns do not show significant mediation. Consequently, organizations should consider implementing privacy protection policies, clear data handling policies, user-control features, and specific, user-focused digital-literacy initiatives, while not just focusing on general security awareness.

6. Conclusion

The study demonstrates that, in the context of social media, there are separate effects of social media usage and of perceived control on privacy and security concerns and behavioral response. The measurement model has proven to be reliable and valid, with Cronbach's α values from .835 to .918, composite reliability values range of .888 to .932, and AVE values are all greater than the recommended value. The structural model also supports that significant relationships exists between SMUI, security awareness and perceived control and privacy/security concerns. The privacy concerns have a significant effect on behavioural responses, while the direct effect of SMUI, security awareness, and perceived control on behavioural response are not significant.

The overall findings indicate that privacy concerns are the most dominant mental pathway that affects users' behaviour. Behavioural responses are not strongly affected by security concerns. The findings of the study thus point to the importance of organizations, platforms and policy makers to improve privacy transparency, augment user control, create effective awareness programmes and implement responsible digital practices. These measures can assist in the adoption of safer and more informed forms of behaviours in increasingly social media rich environments.

References

1. Alsmadi D. et al. Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. Kybernetes. 2024;53(1):451–66.
2. Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, 67(1), 26–53. https://doi.org/10.1111/jcom.12276
3. Bhandari, R. S., Bansal, A., Mathur, S., & Nain, H. (2022). Privacy concern behaviour on social media sites: A comparative analysis of urban and rural users. Global Business Review.
4. Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. Communication Research, 48(7), 953–977. https://doi.org/10.1177/0093650218800915
5. Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. Information, Communication & Society, 20(8), 1261–1278.
6. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690
7. Chanchary, F. H., Abdelaziz, A., & Chiasson, S. (2018). User perceptions of privacy and security in online social networking services. Computers & Security.
8. Christofides, E., Muise, A., & Desmarais, S. (2012). Hey Mom, what's on your Facebook? Comparing Facebook disclosure and privacy in social networking sites. Cyberpsychology, 6(1).
9. Chung, K.-C., Chen, C.-H., Tsai, H.-H., & Chuang, Y.-H. (2021). Social media privacy management strategies: A SEM analysis of user privacy behaviors. Computer Communications, 174, 122–130. https://doi.org/10.1016/j.comcom.2021.04.012
10. Chung, K.-C., Chen, C.-H., Tsai, H.-H., & Chuang, Y.-H. (2021). Social media privacy management strategies: A SEM analysis of user privacy behaviors. Computer Communications, 174, 122–130.
11. Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing the multifaceted nature of privacy-related decision making. Journal of Computer-Mediated Communication, 21(5), 432–449.
12. Dombrowski, J., & Trepte, S. (2026). Taking stock of social media privacy: Meta-analytic evidence on how control, trust, and concerns are associated with social media use, disclosure, and protection. Journal of Computer-Mediated Communication, 31(1).
13. Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x
14. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. J Mark Res. 1981;18(1):39–50
15. Ham, C.-D. (2017). Exploring how consumers cope with online behavioral advertising. International Journal of Advertising, 36(4), 632–658.
16. Jenkins-Guarnieri, M. A., Wright, S. L., & Johnson, B. (2013). The interrelationships among attachment style, personality traits, interpersonal competency, and Facebook connectedness. Psychology of Popular Media Culture, 2(2), 117–125.
17. Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. Computers in Human

Behavior, 107, 106260. https://doi.org/10.1016/j.chb.2020.106260
18. Juma M. et al. Online social network analysis for cybersecurity awareness. Recent Adv Intell Syst Smart Appl.
19. Kaur, H., & Singh, B. (2025). Social media privacy breach of Gen Z: Understanding their traumatic experiences and coping strategies for well-being. Indian Journal of Marketing, 55(9).
20. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002
21. Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. Identity in the Information Society, 2, 39–63. https://doi.org/10.1007/s12394-009-0019-1
22. Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. Journal of Information Technology, 25(2), 109–125. https://doi.org/10.1057/jit.2010.6
23. Lyngdoh, T., Chefor, E., Osakwe, C. N., & others. (2023). Social isolation and social anxiety as drivers of Generation Z's willingness to share personal information on social media. Psychology & Marketing, 40(1), 5–26. https://doi.org/10.1002/mar.21744
24. Makhdoom, I., Abolhasan, M., Lipman, J., & others. (2018). Taxonomy of mobile users' security awareness. Computers & Security, 73, 266–293. https://doi.org/10.1016/j.cose.2017.10.015
25. Mazhar, B., Niu, J., Maqsood, F., Ul Haq, I., & Tareen, H. K. (2026). Decoding the privacy paradox: Moderating effects of privacy concerns on awareness of identity disclosure and protective behaviors on social media. Journal of Social and Personal Relationships.
26. McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lacey, D. (2017). The effect of resilience and social influence on information security awareness and behavioural intentions. Journal of Information Security and Applications, 35, 68–77.
27. McKee, M., Dahl, A. J., & Peltier, J. W. (2024). Gen Z's personalization paradoxes: A privacy calculus examination of digital personalization and brand behaviors. Journal of Consumer Behaviour. https://doi.org/10.1002/cb.2199
28. Monteith S. et al. Increasing cybercrime since the pandemic: concerns for psychiatry. Curr Psychiatry Rep. 2021;23:1–9.
29. Muhammad, S. S., Dey, B. L., Bala, H., et al. (2024). A typology and model of privacy- and security-concerned users' attitudes towards digital footprints and consequent influence on their social media adaptation. Journal of the Association for Information Systems, 25(5), 1240–1273.
30. Muhammad, S. S., Dey, B. L., Bala, H., et al. (2024). A typology and model of privacy- and security-concerned users' attitudes towards digital footprints and consequent influence on their social media adaptation. Journal of the Association for Information Systems, 25(5), 1240–1273.
31. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176.
32. Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. Journal of Applied Developmental Psychology, 30(3), 227–238.
33. Polas MRH, Raju V. Technology and entrepreneurial marketing decisions during COVID-19. Global J Flex Syst Manage. 2021;22(2):95–112.
34. Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. Computers in Human Behavior, 25(2), 578–586.
35. Senthilkumar K, Easwaraamoorthy S. A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP Conf Ser Mater Sci Eng. 2017;263(4):042043.
36. Steinfield, C., Ellison, N. B., & Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. Journal of Applied Developmental Psychology, 29(6), 434–445.
37. Stone, R., & Eveleth, D. (2026). Exploring the privacy-protection behaviors of Generation Z: The role of subjective norms. Information and Computer Security. https://doi.org/10.1108/ICS-07-2025-0282
38. Taddeo, M., & Floridi, L. (2020). The ethics of digital well-being: A thematic review. Science and Engineering Ethics, 26(4), 2313–2343. https://doi.org/10.1007/s11948-020-00213-5
39. van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. Computers in Human Behavior, 78, 283–297.
40. Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communication Monographs, 59(4), 329–349.
41. Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2023). Privacy concern and its consequences: A meta-analysis. Technological Forecasting and Social Change.
42. Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer Affairs, 43(3), 389–418.