Received 16 June 2023
Revised 2 October 2023
28 November 2023
Accepted 4 January 2024

My privacy at risk – my guard is on: a study of SNS use among young adults

Meenakshi Handa, Ronika Bhalla and Parul Ahuja
University School of Management Studies,
Guru Gobind Singh Indraprastha University, New Delhi, India

Abstract

Purpose – Increasing incidents of privacy invasion on social networking sites (SNS) are intensifying the concerns among stakeholders about the misuse of personal data. However, there seems to be limited research on exploring the impact of specific privacy concerns on users' intention to engage in various privacy protection behaviors. This study aims to examine the role of social privacy concerns, institutional privacy concerns and privacy self-efficacy as antecedents of privacy protection–related control activities intention among young adults active on SNS.

Design/methodology/approach – Data collected from 284 young adults active on SNS was analyzed through partial least squares structural equation modeling using Smart PLS.

Findings – The results indicate that institutional privacy concerns, social privacy concerns and privacy self-efficacy positively influence the control activities intention of SNS users. The extent of privacy self-efficacy and privacy protection-related control activities intention differs among users based on gender.

Research limitations/implications – This study is limited to a population of young adults in the age group of 18–25 years.

Practical implications – The findings of this study form the basis for specific recommendations addressing the different types of privacy concerns experienced by social media users, promoting responsible privacy control behaviors on online platforms and discouraging the possible misuse of information by third parties.

Originality/value – This study validates a theoretical framework that can contribute to future investigations concerning the use of SNS. The study findings form the basis for a set of practical recommendations for policymakers, SNS platforms and users.

Keywords Privacy concerns, Privacy protection behavior, Social networking sites, Information disclosure, Young adults

Paper type Research paper

1. Introduction

Social networking sites (SNS) have rapidly become a popular means for members to connect with others, gather information, share their interests and derive entertainment

Funding: The authors received no financial support for the research, authorship and/or publication of this article.

Declaration of conflicting interests: The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

(Boulianne, 2015; Chen, 2018; Pelletier *et al.*, 2020). Users spend an average of 2 h and 27 min daily on SNS (Statista, 2022a). Over time, the content shared by social media users stacks up and can be accessed by others at any time (Zhu and Bao, 2018; Zhang *et al.*, 2023). This has resulted in privacy concerns among users (Chen, 2018). Furthermore, these concerns are accentuated by the increasing incidents of data breaches and privacy intrusion on SNS. According to a survey by GoVerizon, 58% of social media users reported some privacy invasion of their social media accounts (Hutchinson, 2022).

Users are concerned that their personal information available on SNS could be used inappropriately and in an unauthorized manner. The information shared by users online can be used by marketers to profile them (Malhotra *et al.*, 2004). Organizations can access online data to gain information about their job candidates (Drake *et al.*, 2016). Social media platforms can be accessed by cybercriminals, who subsequently sell user information at various hacking forums (Suciu, 2022). Besides, some users report experiencing trolling, cyberbullying and stalking (Kaspersky, 2019). There is concern among SNS users about the unintended use of their personal information by other social media users (Raynes-Goldie, 2010) as well as by the SNS and third-party organizations (Bright *et al.*, 2021).

Increasing incidents of data hacking have led to around 69% of SNS users either deleting or contemplating deleting their accounts (Hutchinson, 2022). This adversely affects the public image and survival of SNS platforms (Krasnova *et al.*, 2009) as users may refuse to use them if the platforms do not take more initiatives to protect user privacy (Milne *et al.*, 2004). However, not all users are likely to be discouraged from SNS usage because of privacy concerns (Bright *et al.*, 2021). Users may adopt privacy protection strategies, such as providing false or incomplete personal information (Youn, 2009) and limiting the visibility of their SNS profiles (Chen, 2018). This is in consonance with the communication privacy management theory (Petronio, 2002). The adoption of privacy protection strategies can be enhanced if users have confidence in their ability to manage the privacy settings of their accounts (Chen, 2018).

Prior research provides an understanding of general privacy concerns (Dinev and Hart, 2004). But there is a need to further explore the influence of specific privacy concerns on users' intention toward controlling their social media activities – a privacy protection behavior undertaken by some users. To address this gap, the present study strives to examine the extent of social privacy concerns, institutional privacy concerns, perceived privacy self-efficacy and privacy control activities intention among young adults and understand the influence of these factors on the control activities intention of users on SNS.

This study contributes to the existing literature in several ways. First, it describes the levels of social privacy concerns, institutional privacy concerns, privacy self-efficacy and the extent of control activities intention among young social media users. Second, it positions control activities intention as a direct outcome of privacy concerns. Third, it explores the impact of users' confidence in their ability to manage privacy settings on their SNS control activities intention.

On one hand, the number of SNS users globally is expected to rise to about 6 billion in 2027 from 4.26 billion in 2021 (Statista, 2023a). On the other hand, there is concern among online users with respect to the security of their online identity (Statista, 2023b). Besides, cybercrime is anticipated to escalate in the years ahead (Statista, 2022b). The occurrences of SNS privacy intrusions can be expected to also rise, thus highlighting a need to better understand the various privacy concerns of the users. The underlying purpose of this study is to help develop strategies for policymakers, social media platforms and social media users that will address the different types of privacy concerns through appropriate policy and

organizational interventions and encourage responsible privacy control behaviors among social media users so as to enable the use of social media platforms with greater security.

2. Literature review

2.1 Privacy concerns and social media

According to Trepte *et al.* (2015, p. 335), online privacy is "the process of controlling access to the self while using internet services." Privacy is not about detaching from others but involves managing one's associations with others (Pedersen, 1997). Newell (1994) posited that when people feel that their well-being is likely to be negatively impacted in a situation, they are likely to seek privacy. Data privacy is an issue of burgeoning concern for various stakeholders, including consumers, organizations and government regulators. Privacy concerns denote users' apprehensions about the risk to their online information, such as the likelihood of data loss because of privacy intrusion (Xu *et al.*, 2013) and information tracking by entities within or outside their social network (Malik *et al.*, 2021). People are concerned about unforeseeable access to the information shared on their SNS accounts, including responses to their activities in the form of comments and messages (Raynes-Goldie, 2010). Users cannot control the further usage of the information as it is available to the whole community and can be accessed, taped and manipulated by others without their permission, and can lead to activities such as identity fraud and social phishing (Shin, 2010).

Apprehensions among SNS members regarding the unauthorized access and use of their information by other users are termed as social privacy concerns (Ozdemir *et al.*, 2017). About 81% of social media users were more apprehensive about their social privacy in 2021 than in the preceding year (Hutchinson, 2022). Social privacy concerns arise from the online social environment of SNS users (Krasnova *et al.*, 2009). People use various loopholes to access social media content not shared with them such as masquerading to pry into the lives of other people (Raynes-Goldie, 2010). Besides, people humiliate SNS users by posting harmful and offensive content about them publicly, which tarnishes their image (Krasnova *et al.*, 2009).

Institutional privacy concerns relate to the unauthorized use of online user information by SNS providers and third parties (Krasnova *et al.*, 2009). About 90% of surveyed users are bothered by social media organizations making money from their data (Hutchinson, 2022). Organizations can access users' personal information and share it with unauthorized entities without obtaining their consent (Milne *et al.*, 2004). Advertisers frequently target their advertisements to online users based on the latter's history of social media activities, because of which users often view those ads for products that they consider but are not really interested in (Logan *et al.*, 2021). In addition, people are also concerned about the vulnerability of their information to government surveillance activities (Wilton, 2017).

Some differences in individuals' level of privacy concerns and their privacy-protection behaviors based on demographic factors have been indicated in previous research. Females are posited as more apprehensive about information privacy than males and are more likely to take necessary protective measures (Mohamed and Ahmad, 2012). Milne *et al.* (2004) suggested that the privacy protection behavior of users increases with schooling.

2.2 Privacy self-efficacy

Despite harboring privacy concerns, users may continue to be active on SNS, thus creating a "privacy paradox" (Norberg *et al.*, 2007). This could be due to perceived privacy self-efficacy, which is "the extent to which users are confident about their abilities to protect themselves from potential threats arising from privacy intrusion" (Cho *et al.*, 2009, p. 404).

Chen and Chen (2015) posited that limiting profile visibility and self-disclosure are favorably affected by self-efficacy in privacy management on SNS.

2.3 Privacy protection behaviors

Users may use different ways to manage their social media privacy, such as using aliases or false names (Raynes-Goldie, 2010), factor authentications and unique passwords for each account (Hutchinson, 2022). Other users may limit their information disclosure or contemplate taking short breaks from social media. Conscious control is the purposeful adjustment of details revealed or information shared by SNS users, which may be due to users' inability to gauge the type of people who will view their information and the resultant uncertainty about data visibility (Krasnova *et al.*, 2009).

Bright *et al.* (2021) observed that privacy protection behaviors are adopted by users to reduce the tracking of their data. Shokouyar *et al.* (2018) suggested that users are more inclined to control their activities on Instagram rather than taking short breaks from its usage or shifting their use to other SNS. Social privacy concerns lower information visibility on user accounts (Young and Quan-Haase, 2013). Users may disclose only what they consider to be innocuous information because of perceived privacy risks (Krasnova *et al.*, 2009). Users are more likely to share false and incomplete details about themselves (Alashoor *et al.*, 2017) while being cautious about the volume and kind of information shared (Krasnova *et al.*, 2009; Youn, 2009). Chen (2018) pointed to the direct positive influence of privacy self-efficacy on self-disclosure, friending and restricting profile visibility.

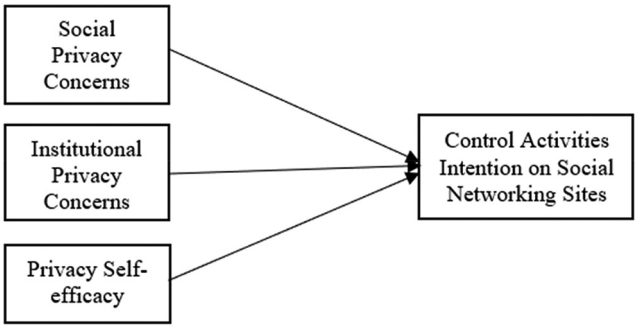
Based on the reviewed literature, the following hypotheses have been taken up for examination in this study:

H1. Social privacy concerns positively impact the control activities intention of young adults on SNS.

H2. Institutional privacy concerns positively impact the control activities intention of young adults on SNS.

H3. Privacy self-efficacy positively impacts the control activities intention of young adults on SNS.

The relationships taken up for examination in the study are presented in Figure 1.



Source: Authors' own work

Figure 1.
Proposed theoretical framework

3. Research methodology

Primary data was collected through a structured questionnaire from 284 SNS users aged 18–25 years, studying in various departments of a state university and an affiliated college in New Delhi, India. This group of internet users was targeted for the present study, as in India, among the various age sections, adults aged 18–25 years comprise the greatest proportion of users of SNS (Statista, 2023c). Adults in this age group are more willing to embrace technology and are also posited to be daily active users of mobile phones, computers and the internet (Patel, 2017).

The items used for measuring the relevant constructs, along with their sources have been presented in Table 1. Furthermore, one open-ended question was asked from the respondents: "If you or any of your acquaintances have experienced privacy invasion of information on social networking sites, then please share the experience if possible."

Construct	Item/s	Source
Control activities intention	1. While sharing something on social networking sites, I will try to be careful about what exactly I am saying about myself 2. I will think carefully how much I reveal about myself on social networking sites 3. I may consciously hold back sharing certain information on social networking sites 4. When engaging on social networking sites, I will care about the kind of information I reveal about myself 5. While expressing myself on social networking sites, I will try to consider who can see the information I share	Adapted from Krasnova *et al.* (2009)
Institutional privacy concerns	1. I am concerned that the social networking sites may use my information for other purposes, e.g., analyzing my activities to derive information about me 2. I am concerned that the social networking sites may share/sell my information to other companies without notifying me or getting my authorization 3. I am concerned that social networking sites are tracking and monitoring all my clicks and actions 4. I am concerned about providing my personal information to social networking sites because it could be used in a way I do not foresee	Adapted from Smith *et al.* (1996)
Social privacy concerns	1. I am concerned that the information I share through social networking sites could be misused by people 2. I am concerned that when I share information with people through social networking sites, they may share it with others whom I do not intend 3. I am concerned that the information I share through social networking sites could be used inappropriately by people 4. I am concerned that the information I share through social networking sites could be used improperly by people 5. I am often concerned that people might take advantage of the information they learn about me through social networking sites	Adapted from Smith *et al.* (1996)
Privacy self-efficacy	1. I have skills to protect my privacy on social networking sites 2. I feel confident about blocking spam or unwanted content on social networking sites 3. I feel I can control my privacy settings on social networking sites 4. I feel confident in managing my personal profiles on social networking sites	Adapted from Chen (2018)

Table 1.
Scale items used in the study

Source: Compiled by authors

4. Data analysis and results

4.1 Respondent demographics

The demographic profile of the respondents comprising 68% males and 32% females, with 64% in the age group of 18–21 years and 36% in the age bracket of 22–25 years is presented in Table 2. Almost 75% of the respondents reported spending more than 1 h every day on the SNS with 15.5% spending more than 5 h. About 23% of respondents reported having experienced some kind of privacy invasion on SNS.

Demographics	Count	%
Gender		
Male	192	67.6
Female	92	32.4
Age (years)		
18–21	182	64.1
22–25	102	35.9
Highest education completed		
10+2	127	44.7
Graduation	119	41.9
Postgraduation	38	13.4
Monthly household income (Rs.)		
Less than 25,000	41	14.4
25,000–50,000	54	19
50,000–1,00,000	67	23.6
1,00,000–1,50,000	29	10.2
More than 1,50,000	54	19
Not reported	39	13.7
Approximate daily time spent on SNS		
Less than 30 min	12	4.2
30–60 min	57	20.1
1–3 h	117	41.2
3–5 h	54	19
More than 5 h	44	15.5
Account privacy setting		
Private	181	63.7
Public	30	10.6
Some private/some public	73	25.7
Noticed privacy policy		
Yes	229	80.6
No	39	13.7
Don't know	16	5.6
Read privacy policy		
Yes	149	65.1
No	74	32.3
Don't know	6	2.6
Privacy invasion experienced on SNS		
Yes	65	22.9
No	131	46.1
Don't know	88	31

Source: Authors' own work

Table 2. Respondent profile ($n = 284$)

4.2 Measurement model

This study examines the proposed research framework by conducting partial least squares structural equation modeling with the help of Smart PLS. The convergent validity and discriminant validity of the measurement model are examined, and then the structural model is assessed. Factor loadings of all the items exceed 0.6 and the values of composite reliability (CR) are above 0.7, Cronbach's alpha are higher than the threshold of 0.7, and average variance extracted (AVE) are more than the minimum limit of 0.5 for all the constructs (Table 3) (Hair *et al.*, 2019).

Discriminant validity evaluated through the Fornell–Larcker correlation matrix (Table 4) indicates that the square root of the AVE value of each construct exceeds their value of correlation with other constructs (Fornell and Larcker, 1981). In addition, heterotrait–monotrait ratio of correlations between constructs is less than 0.9 suggesting that the measurement model has good discriminant validity as presented in Table 5 (Henseler *et al.*, 2015).

Construct	Item/s	Loadings	Cronbach's alpha	CR	AVE
Control activities intention	Intention1	0.777	0.832	0.882	0.599
	Intention2	0.806			
	Intention3	0.735			
	Intention4	0.834			
	Intention5	0.713			
Institutional privacy concerns	Institutional1	0.837	0.832	0.887	0.663
	Institutional2	0.808			
	Institutional3	0.816			
	Institutional4	0.795			
Social privacy concerns	Social1	0.794	0.832	0.882	0.600
	Social2	0.719			
	Social3	0.838			
	Social4	0.809			
	Social5	0.705			
Privacy self-efficacy	Self-efficacy1	0.771	0.724	0.821	0.537
	Self-efficacy2	0.774			
	Self-efficacy3	0.747			
	Self-efficacy4	0.628			

Source: Authors' own work

Table 3. Findings of the measurement model

Construct	Control activities intention	Institutional privacy concerns	Privacy self-efficacy	Social privacy concerns
Control activities intention	0.774			
Institutional privacy concerns	0.524	0.814		
Privacy self-efficacy	0.328	0.248	0.733	
Social privacy concerns	0.376	0.535	0.164	0.775

Source: Authors' own work

Table 4. Discriminant validity – Fornell–Larcker criterion

Construct	Control activities intention	Institutional privacy concerns	Privacy self-efficacy	Social privacy concerns
Control activities intention				
Institutional privacy concerns	0.615			
Privacy self-efficacy	0.388	0.307		
Social privacy concerns	0.448	0.639	0.190	

Source: Authors' own work

Table 5. Discriminant validity – heterotrait–monotrait (HTMT) ratio

4.3 Descriptive statistics

Table 6 presents the descriptive statistics pertaining to the variables under examination. The results of the Mann–Whitney test indicate gender-based differences in the control activities intention and privacy self-efficacy ($p < 0.05$) (Table 7). Females report higher levels of control activities intention as compared with males (Table 8). Privacy self-efficacy among females was higher than that among males. The two groups do not differ with regard to institutional privacy concerns and social privacy concerns ($p > 0.05$).

4.4 Structural model

Table 9 presents the results of the structural model evaluation, including path coefficients, significance values, R^2 value and f^2 effect sizes. Figure 2 indicates the structural model obtained through bootstrapping. Social privacy concerns are found to positively impact control activities intention ($\beta = 0.125, f^2 = 0.017, p < 0.05$). Institutional privacy concerns also positively influence control activities intention ($\beta = 0.406, f^2 = 0.168, p < 0.05$). Privacy self-efficacy favorably impacts control activities intention ($\beta = 0.207, f^2 = 0.060, p < 0.05$). Thus, the results of the study support *H1*, *H2* and *H3*. The influence of institutional privacy concerns on control activities intention is higher than that of privacy self-efficacy and social privacy concerns. Overall, the f^2 effect size of institutional privacy concerns is more than

Construct	Mean	SD
Control activities intention	3.86	0.73
Institutional privacy concerns	3.72	0.87
Social privacy concerns	3.50	0.82
Privacy self-efficacy	3.83	0.72

Source: Authors' own work

Table 6. Descriptive statistics of constructs ($n = 284$)

Variables	Mann–Whitney U	*Z*	*p*-value
Control activities intention	7144.500	−2.617	0.009
Institutional privacy concerns	8571.500	−0.405	0.686
Social privacy concerns	8430.000	−0.623	0.533
Privacy self-efficacy	7160.00	−2.596	0.009

Source: Authors' own work

Table 7. Mann–Whitney *U* test statistics

Variables	Gender	*N*	Mean rank	Sum of ranks
Control activities intention	Male	192	133.71	25,672.5
	Female	92	160.84	14,797.5
Institutional privacy concerns	Male	192	141.14	27,099.5
	Female	92	145.33	13,370.5
Social privacy concerns	Male	192	140.41	26,958
	Female	92	146.87	13,512
Privacy self-efficacy	Male	192	133.79	25,688
	Female	92	160.67	14,782

Source: Authors' own work

Table 8. Mann–Whitney *U* test ranks

0.15, thus indicating a medium f^2 effect size, whereas that of privacy self-efficacy and social privacy concerns was less than 0.15, suggesting a small f^2 effect size (Cohen, 1988). Because the variance inflation factor was less than the benchmark limit of 3, collinearity was not found to be an issue (Hair *et al.*, 2019).

The model has a predictive power of 32.8%, as indicated by the R^2 value. The value of standardized root mean square residual is 0.07 which is close to 0.08 (Hu and Bentler, 1999) and the normed fit index is 0.795, which should have been more than 0.90 indicating a relatively satisfactory model fit (Tabachnick and Fidell, 2013).

The study findings thus indicate that institutional privacy concerns, social privacy concerns and a sense of privacy self-efficacy tend to positively impact an individual's privacy control actions. Furthermore, among the three antecedents taken up for examination, institutional privacy concerns have the highest impact on privacy control behaviors. Almost 23% of the respondents reported experiencing some privacy invasion on

Table 9.
Structural model – bootstrapping results

Independent variables	Path coefficients	Control activities intention *p*-value	R^2	f^2	Evaluation
Social privacy concerns	0.125	0.032	32.8%	0.017	Supported
Institutional privacy concerns	0.406	0.000		0.168	Supported
Privacy self-efficacy	0.207	0.000		0.060	Supported

Source: Authors' own work

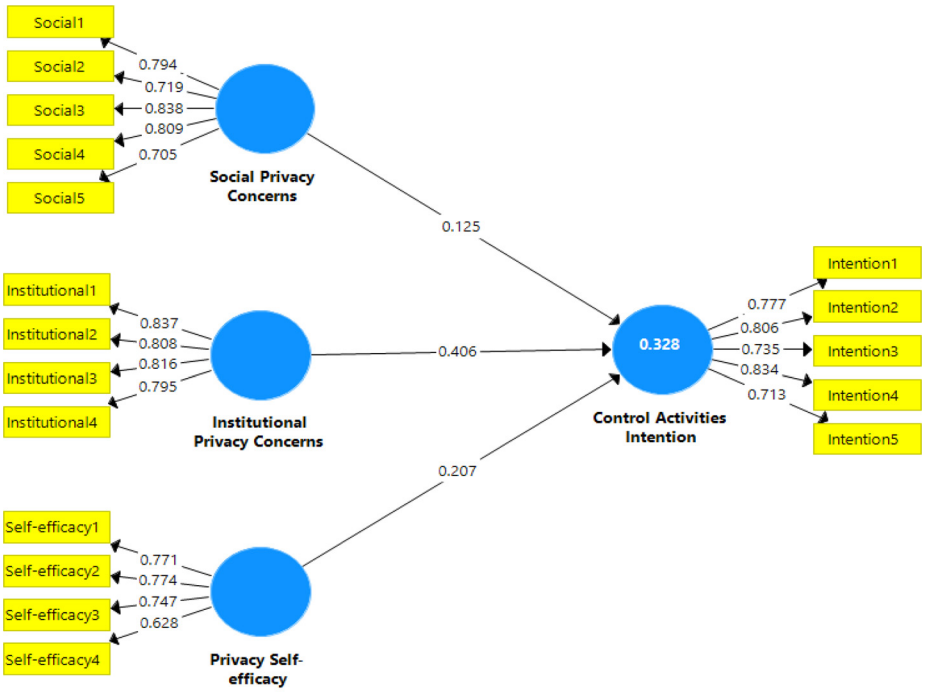


Figure 2.
Structural model

Source: Authors' own work

SNS. In response to the open-ended question regarding experiences, if any, of privacy invasion of information on SNS, several respondents reported incidents of account hacking, impersonation, receiving messages from unknown users to obtain information, stalking and harassment. Also, some respondents mentioned phishing attacks, scams and strange SNS activities, including the sharing of misleading posts on the network.

5. Discussion and implications

The study indicates that the presence of social and institutional privacy concerns among young adult SNS users can lead to a conscious management of the information put online by them as a strategy for handling privacy issues. Thus, those social media users who have higher concerns regarding the intrusion of their social media account's privacy by individuals who are a part of their online network or about the misuse of their private information by SNS providers or organizations are more likely to control and manage their social media activities carefully to protect their privacy. These young adults are more likely to consider the nature, amount and kind of information they will share on SNS. They may purposefully withhold certain information to protect their privacy and may consider the prospective viewers of their content while revealing other information on social media. In addition, the findings indicate a higher level of institutional privacy concerns as compared with social privacy concerns, which may be because of the increasing number of reports regarding incidents of online data breaches (Statista, 2023d), reflecting inadequate management of user data by SNS organizations.

Furthermore, the study indicates that users who believe themselves to be adept at managing the privacy settings of their SNS accounts are more likely to exercise conscious control over their SNS activities as a privacy protection measure. Also, the study finds differences in control activities intention and privacy self-efficacy among respondents based on gender. A section of respondents reported specific incidents of privacy invasion experienced by them or their acquaintances.

5.1 Theoretical implications

The study extends the extant literature on the subject of user privacy concerns and control behavior on SNS. It examines the understudied privacy protection strategies of SNS control activities through the lens of user privacy. The findings of the study inform us about the extent to which the two types of privacy concerns, that is, institutional privacy concerns and social privacy concerns, can cause users to engage in privacy protection measures and provide support for a theoretical framework that can contribute to future investigations concerning the use of SNS and motivate researchers to examine constructs related to SNS users' control activities intentions. Methodologically, the study adapts and validates the measurement scales used in prior research in the Indian context.

5.2 Practical implications

The study has implications for policymakers, social media platforms and social media users. The study findings indicate only moderate levels of privacy concerns among a significant section of the target respondents. Policymakers thus need to make SNS users more aware of the consequences of privacy violations and the need to exercise caution regarding the personal information they share and also about to whom they are giving access to their SNS accounts. Users must be made to appreciate the fact that SNS providers alone cannot manage user privacy and that users themselves also need to exercise vigilance and manage the privacy control features to safeguard their information.

The study indicates that only 65% of users read the privacy policy of the SNS that they are active on. Policymakers and SNS platforms can take more steps to sensitize users about the importance of reading privacy policies. SNS can provide simplified, transparent and summarized versions of their privacy policies that are easy to understand and that inform users about the kind of personal data being collected, its storage location and how and by whom it may be used. Privacy statements and policies can be positioned at noticeable locations on SNS platforms in an attention-getting manner involving images, audio, video and graphics. In addition, SNS platforms can explain in their policy statements the possible advantages of the use of certain personal information by organizations to better serve users, such as personalized product offers. Third-party organizations can also clearly inform users about their privacy policies in terms of how they collect and use data. SNS must seek explicit permissions from users to use their information or to share it with third parties.

Because the findings of the study indicate that users' sense of privacy self-efficacy positively impacts their privacy control intention, efforts must be made to enhance users' confidence in safeguarding their own online privacy. They can be provided with easy-to-exercise privacy controls, such as being able to make posts visible to desired audiences for a limited time span and restricting the audiences who can see the SNS accounts that are a part of the users' SNS network. Users should be offered more options to choose from as to who should get access to their SNS accounts. These privacy control options should be highlighted on the SNS platforms.

Stricter laws and punitive measures need to be implemented to prevent the unauthorized gathering of personal information from SNS and its misuse by third-party institutions. SNS providers must ensure compliance with their privacy rules by third-party organizations that have been given access to their sites. SNS need to be more ethical and vigilant with respect to their use of member information and privacy protection. Appropriate mechanisms need to be designed to strengthen the encryption of data shared on SNS to alleviate the privacy concerns of users. SNS may need to enhance their platform privacy by using numerous layers of firewalls. Besides, they can divide and store user information so that, in the case of infringement of data stored at one location, the remaining user information would stay safe.

Finally, users themselves need to exercise conscious control over the information they are revealing about themselves by considering what and how much is being shared and who can be its potential viewers. They need to be vigilant about third-party apps that may have been given access to their social media accounts by the SNS platforms or by themselves. They need to be watchful of any unusual activity taking place on their social media accounts, which must be immediately reported to the concerned SNS providers and regulators so that they can take the necessary preventive and corrective actions.

References

Alashoor, T., Han, S. and Joseph, R.C. (2017), "Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: an APCO model", *Communications of the Association for Information Systems*, Vol. 41 No. 1, pp. 62-96, doi: 10.17705/1cais.04104.

Boulianne, S. (2015), "Social media use and participation: a meta-analysis of current research", *Information, Communication and Society*, Vol. 18 No. 5, pp. 524-538, doi: 10.1080/1369118X.2015.1008542.

Bright, L.F., Lim, H.S. and Logan, K. (2021), "'Should I post or ghost?': examining how privacy concerns impact social media engagement in US consumers", *Psychology and Marketing*, Vol. 38 No. 10, pp. 1712-1722, doi: 10.1002/mar.21499.

Chen, H.T. (2018), "Revisiting the privacy paradox on social media with an extended privacy calculus model: the effect of privacy concerns, privacy self-efficacy, and social capital on privacy

management", *American Behavioral Scientist*, Vol. 62 No. 10, pp. 1392-1412, doi: 10.1177/0002764218792691.

Chen, H.T. and Chen, W. (2015), "Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection", *Cyberpsychology, Behavior, and Social Networking*, Vol. 18 No. 1, pp. 13-19, doi: 10.1089/cyber.2014.0456.

Cho, H., Rivera-Sánchez, M. and Lim, S.S. (2009), "A multinational study on online privacy: global concerns and local responses", *New Media and Society*, Vol. 11 No. 3, pp. 395-416, doi: 10.1177/1461444808101618.

Cohen, J. (1988), *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed., *Routledge*, New York, NY.

Dinev, T. and Hart, P. (2004), "Internet privacy concerns and their antecedents – measurement validity and a regression model", *Behaviour and Information Technology*, Vol. 23 No. 6, pp. 413-422, doi: 10.1080/01449290410001715723.

Drake, J., Hall, D., Becton, J.B. and Posey, C. (2016), "Job applicants' information privacy protection responses: using social media for candidate screening", *AIS Transactions on Human-Computer Interaction*, Vol. 8 No. 4, pp. 160-184, doi: 10.17705/1thci.00084.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50, doi: 10.2307/3151312.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24, doi: 10.1108/EBR-11-2018-0203.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2015), "A new criterion for assessing discriminant validity in variance-based structural equation modeling", *Journal of the Academy of Marketing Science*, Vol. 43 No. 1, pp. 115-135, doi: 10.1007/s11747-014-0403-8.

Hu, L.T. and Bentler, P.M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives", *Structural Equation Modeling: A Multidisciplinary Journal*, Vol. 6 No. 1, pp. 1-55, doi: 10.1080/10705519909540118.

Hutchinson, A. (2022), "New survey shows that social media users are increasingly concerned about data privacy [infographic]", *Social Media Today*.

Kaspersky (2019), "The true value of digital privacy: are consumers selling themselves short?", *Kaspersky Lab Global Privacy Report 2018*.

Krasnova, H., Günther, O., Spiekermann, S. and Koroleva, K. (2009), "Privacy concerns and identity in online social networks", *Identity in the Information Society*, Vol. 2 No. 1, pp. 39-63, doi: 10.1007/s12394-009-0019-1.

Logan, K., Bright, L.F. and Gangadharbatla, H. (2021), "Exploring the privacy paradox among social media users in the United States", *Journal of Data Protection and Privacy*, Vol. 4 No. 3, pp. 303-321.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336-355, doi: 10.1287/isre.1040.0032.

Malik, A., Dhir, A., Kaur, P. and Johri, A. (2021), "Correlates of social media fatigue and academic performance decrement: a large cross-sectional study", *Information Technology and People*, Vol. 34 No. 2, pp. 557-580, doi: 10.1108/ITP-06-2019-0289.

Milne, G.R., Rohm, A.J. and Bahl, S. (2004), "Consumers' protection of online privacy and identity", *Journal of Consumer Affairs*, Vol. 38 No. 2, pp. 217-232, doi: 10.1111/j.1745-6606.2004.tb00865.x.

Mohamed, N. and Ahmad, I.H. (2012), "Information privacy concerns, antecedents and privacy measure use in social networking sites: evidence from Malaysia", *Computers in Human Behavior*, Vol. 28 No. 6, pp. 2366-2375, doi: 10.1016/j.chb.2012.07.008.

Newell, P.B. (1994), "A systems model of privacy", *Journal of Environmental Psychology*, Vol. 14 No. 1, pp. 65-78, doi: 10.1016/S0272-4944(05)80199-9.

Norberg, P.A., Horne, D.R. and Horne, D.A. (2007), "The privacy paradox: personal information disclosure intentions versus behaviors", *Journal of Consumer Affairs*, Vol. 41 No. 1, pp. 100-126, doi: 10.1111/j.1745-6606.2006.00070.x.

Ozdemir, Z.D., Smith, H.J. and Benamati, J.H. (2017), "Antecedents and outcomes of information privacy concerns in a peer context: an exploratory study", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 642-660, doi: 10.1057/s41303-017-0056-z.

Patel, D. (2017), "10 tips for marketing to gen Z on social media", *Forbes*.

Pedersen, D.M. (1997), "Psychological functions of privacy", *Journal of Environmental Psychology*, Vol. 17 No. 2, pp. 147-156, doi: 10.1006/jevp.1997.0049.

Pelletier, M.J., Krallman, A., Adams, F.G. and Hancock, T. (2020), "One size doesn't fit all: a uses and gratifications analysis of social media platforms", *Journal of Research in Interactive Marketing*, Vol. 14 No. 2, pp. 269-284, doi: 10.1108/JRIM-10-2019-0159.

Petronio, S. (2002), "Boundaries of privacy: dialectics of disclosure", *Choice Reviews Online*, Vol. 40, doi: 10.5860/choice.40-4304.

Raynes-Goldie, K. (2010), "Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook", *First Monday*, Vol. 15 No. 1, pp. 1-4, doi: 10.5210/fm.v15i1.2775.

Shin, D.H. (2010), "The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption", *Interacting with Computers*, Vol. 22 No. 5, pp. 428-438, doi: 10.1016/j.intcom.2010.05.001.

Shokouyar, S., Siadat, S.H. and Razavi, M.K. (2018), "How social influence and personality affect users' social network fatigue and discontinuance behavior", *Aslib Journal of Information Management*, Vol. 70 No. 4, pp. 344-366, doi: 10.1108/AJIM-11-2017-0263.

Smith, H.J., Milberg, S.J. and Burke, S.J. (1996), "Information privacy: measuring individuals' concerns about organizational practices", *MIS Quarterly: Management Information Systems*, Vol. 20 No. 2, pp. 167-195, doi: 10.2307/249477.

Statista (2022a), "Daily social media usage worldwide", *Statista Research Department*, available at: www.statista.com/statistics/433871/daily-social-media-usage-worldwide/ (accessed 29 June 2022).

Statista (2022b), "Cybercrime expected to skyrocket in coming years", *Statista Research Department*, available at: www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ (accessed 28 June 2023).

Statista (2023a), "Number of social media users 2025", *Statista Research Department*, available at: www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (accessed 18 November 2023).

Statista (2023b), "Worldwide internet user attitudes regarding online identity theft as of January 2023", *Statista Research Department*, available at: www.statista.com/statistics/296700/personal-data-security-perception-online/ (accessed 28 November 2023).

Statista (2023c), "Use of social media platforms among people in India as of January 2022, by age group", *Statista Research Department*, available at: www.statista.com/statistics/1388571/india-social-media-usage-by-age-group/ (accessed 22 August 2023).

Statista (2023d), "Use of social media platforms among people in India as of January 2022, by age group", *Statista Research Department*, available at: www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/#:~:text=Thelargestreporteddataleakage,databreach%2Coccurredin2013 (accessed 27 November 2023).

Suciu, P. (2022), "Social media user information for sale on the dark web", *Forbes*.

Tabachnick, B.G. and Fidell, L.S. (2013), "Using multivariate statistics", *Pearson Education*, Vol. 6, doi: 10.1515/snde-2014-0102.

Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A. and Lind, F. (2015), "Do people know about privacy and data protection strategies? Towards the 'online privacy literacy

scale (OPLIS)"', in Gutwirth, S., Leenes, R. and de Hert, P. (Eds), *Reforming European Data Protection Law*, Springer, Netherlands, doi: 10.1007/978-94-017-9385-8_14.

Wilton, R. (2017), "After Snowden – the evolving landscape of privacy and technology", *Journal of Information, Communication and Ethics in Society*, Vol. 15 No. 3, pp. 328-335, doi: 10.1108/JICES-02-2017-0010.

Xu, F., Michael, K. and Chen, X. (2013), "Factors affecting privacy disclosure on social network sites: an integrated model", *Electronic Commerce Research*, Vol. 13 No. 2, pp. 151-168, doi: 10.1007/s10660-013-9111-6.

Youn, S. (2009), "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents", *Journal of Consumer Affairs*, Vol. 43 No. 3, pp. 389-418, doi: 10.1111/j.1745-6606.2009.01146.x.

Young, A.L. and Quan-Haase, A. (2013), "Privacy protection strategies on Facebook: the internet privacy paradox revisited", *Information Communication and Society*, Vol. 16 No. 4, pp. 479-500, doi: 10.1080/1369118X.2013.777757.

Zhang, Y., Luo, C., Wang, H., Chen, Y. and Chen, Y. (2023), "'A right to be forgotten': retrospective privacy concerns in social networking services", *Behaviour and Information Technology*, Vol. 42 No. 7, pp. 1-22, doi: 10.1080/0144929X.2022.2046162.

Zhu, X. and Bao, Z. (2018), "Why people use social networking sites passively: an empirical study integrating impression management concern, privacy concern, and SNS fatigue", *Aslib Journal of Information Management*, Vol. 70 No. 2, pp. 158-175, doi: 10.1108/AJIM-12-2017-0270.

Further reading

Gao, W., Liu, Z., Guo, Q. and Li, X. (2018), "The dark side of ubiquitous connectivity in smartphone-based SNS: an integrated model from information perspective", *Computers in Human Behavior*, Vol. 84, pp. 185-193, doi: 10.1016/j.chb.2018.02.023.

Jiang, Z., Heng, C.S. and Choi, B.C.F. (2013), "Privacy concerns and privacy-protective behavior in synchronous online social interactions", *Information Systems Research*, Vol. 24 No. 3, pp. 579-595, doi: 10.1287/isre.1120.0441.

Li, J., Guo, F., Qu, Q.-X. and Hao, D. (2022), "How does perceived overload in mobile social media influence users' passive usage intentions? Considering the mediating roles of privacy concerns and social media fatigue", *International Journal of Human–Computer Interaction*, Vol. 38 No. 10, pp. 983-992, doi: 10.1080/10447318.2021.1986318.

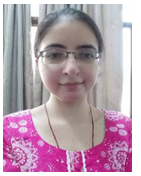
Logan, K., Bright, L.F. and Grau, S.L. (2018), "'Unfriend me, please!': social media fatigue and the theory of rational choice", *Journal of Marketing Theory and Practice*, Vol. 26 No. 4, pp. 357-367, doi: 10.1080/10696679.2018.1488219.

Mousavi, R., Chen, R., Kim, D.J. and Chen, K. (2020), "Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory", *Decision Support Systems*, Vol. 135, pp. 1-14, doi: 10.1016/j.dss.2020.113323.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A. and Buchanan, T. (2007), "Internet users' perceptions of 'privacy concerns' and 'privacy actions'", *International Journal of Human-Computer Studies*, Vol. 65 No. 6, pp. 526-536, doi: 10.1016/j.ijhcs.2006.12.001.

About the authors

Meenakshi Handa has recently retired as a Professor of Marketing from the University School of Management Studies, Guru Gobind Singh Indraprastha University, New Delhi, India, where she taught the marketing core course and elective classes in consumer behavior, services marketing and retail management. She holds over 29 years of teaching, research and industry experience. She has a number of publications in reputed national and international journals. Her areas of research interest span emerging issues in consumer behavior including a focus on consumer adoption of and interface with technology, sustainability and consumer behavior, ethical issues in marketing, services marketing and nonprofit marketing.



Ronika Bhalla is a Research Scholar at University School of Management Studies, Guru Gobind Singh Indraprastha University, New Delhi, India. She has qualified the University Grants Commission National Eligibility Test. Her areas of research interest include sharing economy, sustainability and consumer adoption of digital technologies. She has presented research papers in several national and international conferences. Ronika Bhalla is the corresponding author and can be contacted at: ronikabhalla@gmail.com

Parul Ahuja is a Research Scholar at University School of Management Studies, Guru Gobind Singh Indraprastha University, New Delhi, India. She is presently working as an Assistant Professor in Maharaja Agrasen Institute of Management Studies, affiliated to Guru Gobind Singh Indraprastha University. She has published articles in ABDC, Scopus and Web of Science indexed journals and also attended various international and national conferences.