The Interplay Between Privacy, Trust and Self-disclosure on Social Networking Sites

Eli Fianu, Kwame Simpe Ofori, Richard Boateng, George Ampong

The interplay between privacy, trust and self-disclosure on social networking sites

Eli Fianu[1], Kwame Simpe Ofori [2], Richard Boateng [3], George Oppong Appiagyei Ampong[4]
[1] College of Law and Management Studies, University of KwaZulu Natal
efianu@gmail.com
[2] Department of Computer Science, Ho Technical University
kwamesimpe@gmail.com
[3] University of Ghana Business School
richboateng@ug.edu.gh
[4] Department of Management, Ghana Technology University College
gampong@gtuc.edu.gh

Abstract. Social Networking Sites (SNSs) have become an essential part of the daily lives of billions of people worldwide. Because SNS service providers use a revenue model that relies on data licensing (selling of user data), they share user data with other parties such as government institutions and private businesses. Sharing of user data to third parties raises several privacy concerns. Apart from privacy issues emanating from SNSs sharing user information with third parties, privacy issues may also emanate from users sharing information with SNS members. This study is motivated by the researchers' interest in investigating self-disclosure amongst Ghanaians especially from the perspective of privacy and trust primarily because of recent reports of revenge pornography and other self-disclosure related privacy violations on SNSs in Ghana. A survey was conducted on 523 students from three private universities in Ghana. Out of the 523 questionnaires administered, 452 were validated for analysis. Data collected from the survey was analyzed using the Partial Least Square approach to Structural Equation Modeling (PLS-SEM) performed on SmartPLS Version 3. Results of the study show that privacy awareness, privacy invasion experience, and privacy-seeking behavior have a significant effect on trust in SNS members. Privacy concern was found not to have a significant effect on trust in SNS members. Privacy awareness, privacy concerns, privacy invasion experience, and privacy-seeking behavior were found to have a significant effect on trust in the SNS service provider. Trust in SNS members and trust in the SNS service provider were found to have a significant effect on SNS self-disclosure. Theoretical and practical implications of the study are also discussed.

Keywords: Social Networking Sites, Privacy, Trust, Self-disclosure, Structural Equation Modelling

1. Introduction

Social Networking Sites (SNSs) are generally described as Internet-based applications that allow users to construct and share a personalized profile and lists of confirmed contacts with others on the site. SNSs allow users to see, browse, and communicate with their online friends as well as with friends of other users in the user's online community [1]. SNSs have become an essential part of the daily lives of billions of people worldwide [2].

Self-disclosure is a process of interaction by which a person discloses information about himself or herself to another person [3]. Self-disclosure is a predominant part of social networking because SNS users share a lot of personal information on SNSs. Due to the fast-growing popularity and usage of SNSs, there has been a tremendous rise in the information given out by SNS users [4]. Also, due to the high volumes of content shared by users on SNSs, concerns have been raised about the vulnerability of users with regards to content sharing [5].

SNSs collect and store user browsing data, personal information, as well as distributed content for an unlimited amount of time [6]. Owing to the fact that SNSs use a revenue model that relies on data licensing (selling of user data), they make user data available to other parties, including governmental agencies and business partners [5,6]. Once user information is made available to third parties, users lose control of this information.

Apart from privacy issues emanating from SNSs sharing user information with third parties, privacy issues may also emanate from users sharing information with SNS members. SNS users fear that their posts will be exposed or abused by others [7, 8]. For users, as online social networks grow, the probability of engaging with new contacts also grows, likewise the probability of experiencing negative relationships that may give rise to social overload [9]. SNS users' private information provided during the registration for SNS accounts may become exposed to several parties, leading to possible misuse [10].

Ghana has experienced tremendous growth in SNS usage [11]. Ghana recorded a 22% annual growth of social media users from January 2017 to January 2018, the fourth highest in the world; the global growth rate was 13% [12]. In recent times, Ghana has experienced instances of revenge pornography on SNSs such as Whatsapp and Twitter. Revenge pornography is a class of online pornography that comprises of unprofessional images or videos that were home-made with the approval of those shown, but then later circulated without their approval [13]. There is an aspect of self-disclosure in revenge pornography because victims share private pictures and videos with people they initially trust.

One will expect that these incidents of revenge pornography will deter SNS users in Ghana from self-disclosing private images or videos, but more recent happenings suggest otherwise. Apart from revenge pornography, there have been several reports of other forms of self-disclosure related privacy violations on SNSs in Ghana, such as fraud-related identity theft. This study is motivated by our interest in investigating self-disclosure amongst Ghanaians, especially from the perspective of privacy and

trust mostly because of recent reports of revenge pornography and other privacy violations on SNSs in Ghana.

1 Literature review

1.1 Self-disclosure, Privacy, and Trust on SNSs

Communication Privacy Management (CPM) theory was developed by Sandra Petronio in 1991. It is a theory proposed to generate an empirical understanding of how people make decisions on disclosing and hiding private information [14]. From the perspective of CPM, self-disclosure involves the setting of rules by people when they have to decide whether to reveal or conceal personal information [15]. In effect, the individual controls the disclosure of personal information based on the rules set, and by setting privacy boundaries. Privacy boundaries can vary from fully open to fully closed [14, 16].

Fully open boundaries can be described as situations where an individual discloses information vocally or online to everybody who wants access to it. On the other hand, closed boundary individuals are sceptical about revealing information, hence, they are very careful. During interactions, people usually move between open and closed boundaries, depending on the nature of the relationship between the individuals communicating [14]. CPM proposes that individuals set privacy rules during communication; privacy rules determine what the individual will disclose or not. These privacy rules depend on several factors such as gender, cultural values, and a person's conviction about what is private or not private [14]. Privacy rules are also influenced by assessments of risk-benefits, as well as changes in situational circumstances, for instance, the changes that occur when there is a separation between couples [14]. When a couple separate, they will most likely not use the same privacy rules they had when they were a couple [14].

CPM proposes the phenomenon of boundary turbulence [14]. According to CPM, co-ownership of private information occurs when an individual shares private information with a confidant. If the two individuals who co-own the private information do not negotiate their jointly held privacy rules, there is the likelihood of "boundary turbulence", which means that there are disruptions in the way that co-owners regulate the flow of private information to third parties [14]. Boundary turbulence occurs when a co-owner deliberately destroys the synchronized boundary of privacy to reveal private information [14]. One can, therefore, deduce from CPM that the revealer places some trust in the confidant while disclosing personal information with the hope that there will not be boundary turbulence. Consequently, before an individual will share private information with a confidant, certain expectations come to play. These expectations of confidentiality and responsibility must be met before the sharing of private information. "If you meet my expectations of confidentiality and responsibility, I will share my private information with you, and vice versa" [16].

In order to prevent conflict and unwanted breaches of confidentiality, original owners of information should discuss their expectations of co-ownership of infor-

mation with confidants [16]. The boundary surrounding private information should be managed by mutually negotiated and agreed-upon privacy rules [17].

SNS use for most people is fueled by their desire to be entertained and to pass time [18]. While passing time on SNSs, SNS users are entertained by the active sharing of content (images and videos) as well as synchronous interactions via instant messaging. The amount of pleasure and amusement experienced by SNS users depends on satisfactory associations and trust building. Self-disclosure on SNSs is therefore influenced by satisfactory relationships based on enjoyment, connectedness, and SNS flow experience, as well as perceived risks [18–21].

Self-disclosure in SNSs can be affected by SNS members' perceptions of the safety of their personal information with respect to the service provider [22]. Users are likely not to have a happy experience with SNS use when they have anxieties about the sharing of private information. Awareness of the credibility of a company may reduce one's privacy concerns over self-disclosure or perceived privacy risk; in other words, the more reputable the SNS provider is, the more likely it is that users will disclose personal information [23–26].

In summary, self-disclosure on SNSs is multifaceted. Self-disclosure on SNSs depends largely on user enjoyment of interactions on the SNS, perceived risks, as well as perceptions of how personal information is handled by SNS service providers [27–30].

Regarding online social networking, privacy awareness refers to a person's attention and understanding in terms of various aspects of privacy while using social media platforms [31–33]. Initial SNS studies showed that most SNS users had little knowledge of how their personal information was treated and used, however recent studies show an increase in privacy awareness among SNS users [34]. While increased privacy awareness has been found to reduce trust and information disclosure in e-commerce settings, the opposite holds true for SNSs [34]. Notwithstanding the enhanced level of privacy awareness among SNS users, activities on the SNS platforms keep increasing, which could be attributed to trust in the platforms [4].

Privacy invasion experience describes privacy violations a user might have personally experienced in the past [35]. Humor creation among friends on online social networks may lead some individuals to expose people's private information such as that which exposes their previous improper behavior, mischief, or clumsiness. This exposure may be a playful tease, but the individual whose information is exposed may be offended by the involuntary exposure. Prior privacy invasion experience negatively affects trust and further information disclosure [36].

Privacy-seeking behavior refers to the things people do to protect their information [37]. From the perspective of CPM theory, to protect one's privacy, a person would set privacy boundaries during interaction with people. Privacy boundaries are set based on trust; open when there is trust and closed when there is no trust [16]. Privacy-seeking behavior increases transactional avoidance and subsequent self-disclosure [33].

By definition, trust is the readiness to accept susceptibility based upon optimistic outlooks about another's behavior [38]. Trust theory proposes that trust, which shows a readiness to accept susceptibility based on an optimistic outlook toward another

participant's imminent behavior, has a substantial effect on the behavioral intention of users of services [39]. Trust can be categorized as online or offline [40]. Online trust varies from offline trust because in an online setting, trust issues emanate from both the SNS technology and the SNS service provider. Therefore, it is difficult for internet users to keep a high level of trust for the websites. The internet is mostly viewed as a precarious territory; therefore, online trust is rather tough to achieve and sustain when compared to trust in an offline setting [40].

Interaction creates prospects for people to become acquainted, to form online communities, and to build trust [41]. Trust has been found to have a mediating effect on privacy concerns and information disclosure [42]. Self-disclosure has been a prevalent behavior of SNS users, which arguably motivated previous research to focus on the drivers and inhibitors of self-disclosure. From the perspective of a person using an SNS, ownership rules have an influence on an individual's actions with respect to trust in a "third-party disclosure" of the shared information; we co-own shared private information and so we must be responsible co-owners [43].

SNS providers must assure users of the safety of their personal information during registration for service, especially from the activities of third parties [44]. Privacy seals are issued by a third-party organization (for instance TRUSTe) to show that a site's privacy framework and processes are accredited by them. TRUSTe offers services to assist organizations to revise their privacy management procedures so that they conform to government laws and best practices. Both privacy guidelines and seals may help develop users' trust and assuage their privacy concerns [44]. Previous literature has shown that people may demonstrate more trust in websites that disclose their privacy policies [45–49]. Online trust can, therefore, be seen from the perspective of the SNS provider and SNS members.

Default SNS privacy settings allow users to see each other's profiles either through a one-on-one connection or through a closed or open user group [50]. This default setting (especially on Facebook) also implies that when for instance, A is a friend of B on the SNS, C who is a friend of B can view A's profile even though A and C are not direct friends. Thus, if users maintain the default SNS settings, they may not be aware that people who are not their friends have access to their profile (because of visibility). Consequently, users may eventually share information with people they did not intend sharing the information with. It is therefore imperative that users adjust their privacy settings in SNSs to suit their privacy rules and boundaries [51].

Unwanted privacy breaches could occur even if a user has the most restricted privacy settings [52]. For instance, with Facebook, a user's privacy is influenced by the privacy settings of their friends because if a user has restricted settings, but the friends do not have restricted settings, other people will have access to the user's information. Additionally, in cases where the user removes his/her posts from the SNS (for example Facebook), the posts may still be accessible because of the ease at which information can be saved, shared, and reposted [34]. Another issue of interest in SNSs is the activity stream. An activity stream is a thread that displays every activity of the user (e.g., posts and likes). Activity streams have raised privacy concerns among SNS users because a user might not know all the activities that are included in their activity stream. Users may also not know the people who have access to their activity

stream [34]. Hence, the failure to successfully control who has access to one's information online can create discomfort for SNS users.

2 Research model and hypotheses development

We develop hypotheses mainly from CPM theory and trust theory. We also refer to previous studies that have investigated the hypothesized relationships. The current study seeks to investigate three major variables namely self-disclosure, privacy and trust. Self-disclosure and privacy are inherent in CPM theory, while trust is inferred from CPM theory. To prevent parsimony while investigating these three variables, we combine CPM theory and trust theory to formulate our research model. The hypotheses are stated in the next sections.

Privacy awareness: Based on CPM theory, we argue that awareness of the privacy structure of SNSs (especially privacy settings) allows an individual to set privacy rules when disclosing information to the SNS service provider and other SNS members. When individuals are confident that there is no likelihood of boundary turbulence, they will have trust in the SNS service provider and other SNS members. Privacy awareness, therefore, has a positive effect on trust in the SNS service provider and other SNS members. In a study to determine the impact of privacy, trust and user activity on intentions to share Facebook photos, Malik, Hiekkanen, Dhir, & Nieminen [33] found that privacy awareness had a significant positive effect on trust in the Facebook platform. Facebook users with high privacy awareness tend to exhibit greater levels of trust in the service and are more active [4, 53].

In line with the findings of Malik, Hiekkanen, Dhir, & Nieminen [33], O'Bien & Torres [53], and Stutzman et al. [4] we posit that:

Hypothesis 1. Privacy awareness has a significant positive effect on trust in SNS members

Hypothesis 2. Privacy awareness has a significant positive effect on trust in SNS service provider

Privacy concern: From CPM theory we posit that privacy concern (user apprehension to disclose information) has the tendency to cause an individual to set privacy rules during interactions to prevent boundary turbulence. The higher the apprehension, the less the trust in the SNS service provider and other SNS members. Privacy concern, therefore, has a negative effect on trust in the SNS service provider and other SNS members. In the SNS setting, privacy concern is one of the key factors that affect trust in the service, as well as the intention to disclose information [53,54]. Privacy concern has a negative influence on trust in Facebook and consequently, lower intentions to use Facebook [53]. Also, following CPM theory, we posit that privacy concern has the tendency to cause an individual to set privacy rules during interactions to prevent boundary turbulence. Privacy concern, therefore, influences trust.

In line with theory and the findings of O'Bien & Torres [53] and Proudfoot et al. [54], as well as the tenets of CPM, we posit that:

Hypothesis 3. Privacy concern has a significant negative effect on trust in SNS members
Hypothesis 4. Privacy concern has a significant negative effect on trust in SNS service provider

Privacy invasion experience: We posit (From CPM theory) that when one experiences privacy invasion, there is boundary turbulence which in turn affects trust. Prior privacy experience will therefore negatively influence trust in the SNS service provider and other SNS members; the greater the impact of the experience, the lesser the level of trust. Prior privacy invasion increases perceptions of online privacy risks, which in turn influences trust in SNSs, that is, trust in the SNS service provider and SNS members as well [55]. Prior experience of privacy invasion on SNSs affects trust in SNSs and motivates an individual to alter his/her privacy settings [56]. The victims of online privacy attack tend to appreciate the grave outcomes of privacy loss; their prior experience influences their trust in SNSs [57].

Therefore, in support of the above-mentioned authors and the tenets of CPM, we posit that:

Hypothesis 5. Privacy invasion experience has a significant negative effect on trust in SNS members
Hypothesis 6. Privacy invasion experience has a significant negative effect on trust in SNS service provider

Privacy-seeking behavior: Similar to privacy awareness, based on CPM theory, we argue that when exploring the privacy settings of the SNS allows an individual to set privacy rules when disclosing information to the SNS service provider and other SNS members. When individuals are confident that there is no likelihood of boundary turbulence, they will have trust in the SNS service provider and other SNS members. Privacy awareness, therefore, has a positive effect on trust in the SNS service provider and other SNS members. In a study to determine the impact of privacy, trust and user activity on intentions to share Facebook photos, Malik, Hiekkanen, Dhir, & Nieminen [33] found that privacy-seeking behavior had a significant positive effect on Facebook usage activity. The extent to which SNS users pursue privacy protection strategies will positively affect their trust in the service and their actual activity [4,56,58].

In line with theory and the above findings, we posit that:

Hypothesis 7. Privacy-seeking behavior has a significant positive effect on trust in SNS members
Hypothesis 8. Privacy-seeking behavior has a significant positive effect on trust in SNS service provider

Trust in SNS members and Trust in SNS service provider: Based on trust theory, we posit that an individual who trusts the SNS service provider and other SNS members is ready to accept susceptibility (based on an optimistic outlook), and therefore will be willing to disclose personal information. Furthermore, following CPM theory, we posit that when one trusts the would-be confidant, it implies the would-be confidant meets the needed expectations (of confidentiality) for self-disclosure, hence personal information is likely to be given out, and vice versa. Trust, therefore, positively influences self-disclosure. In a study on the prediction of college students' self-disclosure on Facebook, Chang & Heo [5] found that trust in Facebook had a significant positive effect on the disclosure of personal information on the platform. A study by Malik et al. [33] showed that trust positively impacts users' intentions to share photos on Facebook. Wu, Huang, Yen, & Popova [59] in a study to investigate the effect of online privacy policy on consumer privacy concern and trust found out that trust has a positive impact on willingness to provide personal information.

In line with the above findings and the tenets of CPM theory, we hypothesize that:

Hypothesis 9. Trust in SNS members has a significant positive effect on self-disclosure
Hypothesis 10. Trust in SNS service provider has a significant positive effect on self-disclosure

The proposed research model is shown in Fig. 1

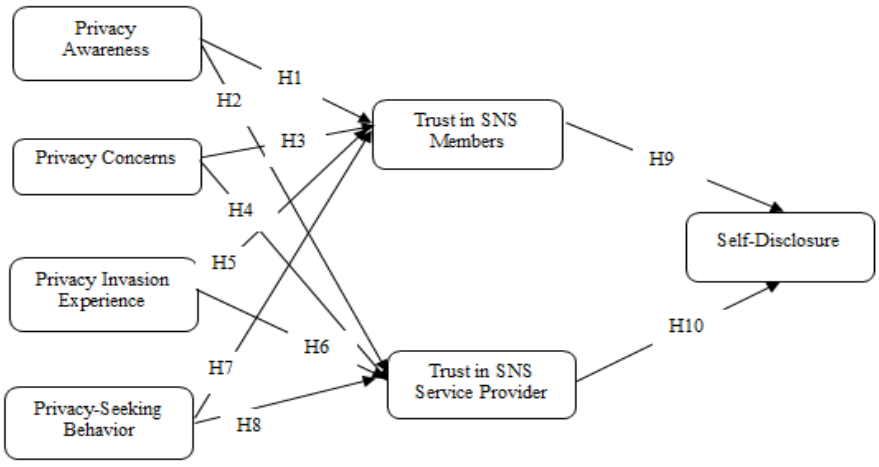

Fig. 1. The proposed research model

3 Methodology

3.1 Instrument development, Sampling and Data Collection

In order to improve content validity, measurement items for the latent variables used in the current study were adopted from previous literature [60]. These items were however reworded to fit the context of social networking sites. Items for Privacy Awareness, Privacy Concerns and Privacy Seeking behavior were adopted from Malik et al. [33]. Privacy Invasion Experience, Trust in SNS members, Trust in SNS service provider and Self Disclosure were all measured with items derived from Cheung, Lee, and Chan [61]. All measurement items were measured using a 5-point Likert scale anchored between strongly disagree (1) and strongly agree (5). Over a five-day period, survey data was collected from 452 respondents, all of whom were students.

4 Results

Data analysis was conducted using the Partial Least Square approach to Structural Equation Modelling (PLS-SEM) performed on SmartPLS Version 3. The PLS-SEM technique is appropriate because it allows for the testing of the relationships between latent constructs in a proposed research model. The current study used the PLS approach since an initial study of the data collected revealed that the data was non-normal. Also, the PLS method is more appropriate since our model is quite new and untested.

4.1 Measurement assessment

The measurement model was assessed based on reliability, discriminant validity and convergent validity. Cronbach's alpha and composite reliability were used to test the reliability of the constructs. Henseler, Ringle, and Sinkovics [62] suggest a threshold of 0.7. It is evident from Table 1 that measurement model is reliable. Convergent validity was also assessed using the average variance extracted (AVE), Henseler et al. [63] recommended that the AVE for each construct should be greater than 0.5 for convergent validity to be assured. Clearly from Table 1 is can be confirmed that convergent validity is assured. Finally, discriminant validity was assessed using the Fornell-Larker criterion [64], and the Heterotrait-Monotrait ratio of correlation [65]. Evidence from Table 2 shows that the square root of the AVEs for each construct is greater than the cross-correlation with other constructs. Also, the results of the HTMT0.85 criterion shown in Table 2 confirm discriminant validity. Overall, the results showed that the psychometric properties of the measures used in the study were satisfactory.

Table 1. Factor Loading and Reliability Statistics.

	Factor Loadings	A	C.R	A.V.E
PA1	**0.822**			
PA2	**0.859**			
PA3	**0.880**	0.912	0.932	0.695
PA4	**0.792**			
PA5	**0.812**			
PA6	**0.833**			
PC1	**0.914**			
PC2	**0.912**			
PC3	**0.880**	0.932	0.948	0.786
PC4	**0.828**			
PC5	**0.896**			
PIE1	**0.941**	0.870	0.939	0.885
PIE2	**0.940**			
PSB1	**0.803**			
PSB2	**0.867**	0.826	0.882	0.652
PSB3	**0.806**			
PSB4	**0.748**			
SD1	**0.811**			
SD2	**0.820**			
SD3	**0.813**	0.833	0.888	0.665
SD4	**0.817**			
TM1	**0.832**			
TM2	**0.874**			
TM3	**0.880**			
TM4	**0.868**	0.929	0.944	0.738
TM5	**0.849**			
TM6	**0.851**			
TP1	**0.797**			
TP2	**0.860**			
TP3	**0.862**			
TP4	**0.866**	0.921	0.938	0.717
TP5	**0.846**			
TP6	**0.847**			

Table 2. Testing Discriminant Validity using the Fornell-Larcker Criterion.

	Fornell Larcker							HTMT						
	PA	PC	PIE	PSB	SD	TM	TP	PA	PC	PIE	PSB	SD	TM	TP
PA	**0.83**													
PC	-0.24	**0.89**						0.26						
PIE	-0.27	0.29	**0.94**					0.31	0.33					
PSB	0.2	0.13	-0.04	**0.81**				0.23	0.16	0.05				
SD	0.44	-0.36	-0.31	0.14	**0.82**			0.5	0.4	0.36	0.17			
TM	0.41	-0.21	-0.4	0.18	0.34	**0.86**		0.44	0.22	0.44	0.18	0.38		

TP	0.58	-0.32	-0.42	0.23	0.42	0.46	**0.85**	0.63	0.34	0.47	0.26	0.48	0.5

Note: Square roots of average variances extracted (AVEs) shown on the first diagonal in bold

4.2 *Structural Model Assessment.*

The structural model was assessed based on the sign, magnitude and significance of the path coefficients of each hypothesized path. The significance of the path coefficients in the structural model was tested using a bootstrap resampling technique with 5000 subsamples drawn with replacement. Results of the assessment of the structural model are shown in Table 3. Apart from the path between Privacy Concern and Trust in Members, all the paths that were earlier hypothesized were found to be significant. About 56 per cent of the variance in the target variable (Self Disclosure) was explained by our model. To assess model fit in PLS we used the standardized root mean square residual (SRMR). The SRMR value for the model was 0.041; a value of less than 0.08 is generally considered a good fit [66]. This value indicates that the structural model exhibits a good fit.

Table 3. Hypotheses testing

Hypotheses	Path	$\hat{\beta}$	T Statistics	P Values	Results
H1	PA →TM	0.291	5.441	0.000	Supported
H2	PA → TP	0.445	10.528	0.000	Supported
H3	PC → TM	-0.075	1.724	0.085	Not Supported
H4	PC → TP	-0.164	4.147	0.000	Supported
H5	PIE→ TM	-0.290	6.347	0.000	Supported
H6	PIE → TP	-0.245	5.776	0.000	Supported
H7	PSB → TM	0.120	2.763	0.006	Supported
H8	PSB → TP	0.149	3.464	0.001	Supported
H9	TM →SD	0.181	3.605	0.000	Supported
H10	TP → SD	0.339	6.865	0.000	Supported
Model fit					
SRMR = 0.041					
$R^2 = 0.56$					

5 Discussions

The current study sought to investigate self-disclosure on SNSs from the perspective of trust and privacy. As mentioned earlier, the researchers treated trust as a two-dimensional variable; trust in SNS provider and trust in SNS members, mainly because the invasion of SNS users' privacy is likely to be caused by these two variables.

The researchers captured privacy of the SNS user in terms of privacy awareness, privacy concerns, privacy invasion experience, and privacy-seeking behavior.

Results of the study show that privacy awareness, privacy invasion experience, and privacy-seeking behavior have a significant effect on trust in SNS members. Privacy concern was found not to have a significant effect on trust in SNS members. Privacy awareness, privacy concerns, privacy invasion experience, and privacy-seeking behavior were found to have a significant effect on trust in the SNS service provider. Trust in SNS members and trust in the SNS service provider were found to have a significant effect on SNS self-disclosure. Nine of the ten hypotheses were supported, which, significantly supports our research model.

Our study provides support for studies conducted by Malik, Hiekkanen, Dhir, & Nieminen [33], O'Bien & Torres [53], and Stutzman et al. [4] which show that, in SNS settings, privacy awareness has a significant effect on trust. This finding shows that when SNS users in Ghana understand and pay attention to privacy issues, it affects the trust they have in the SNS provider as well as other SNS members. The positive relationship between privacy awareness and the trust constructs implies that when SNS users in Ghana are aware of the privacy implications of using the sites, they are likely to build more trust in the sites, that is, knowing and understanding the privacy statements and privacy settings of the SNS is likely to build trust in the SNS. Knowledge of user privacy rights and responsibilities is also likely to result in increased trust in the SNS [67]. This result also implies that SNS service providers can build more trust in SNS users if they find ingenious ways of exposing SNS users to the privacy framework of the sites.

Privacy concern was found to have a significant negative effect on trust in the SNS provider, but a non-significant effect on trust in the SNS members. This finding implies that the there is a high likelihood that Ghanaian SNS users are of the view that their concern for the manner in which their private information and information they submit on SNSs is managed does not influence their trust in SNS members, but influences their trust in the SNS provider. We argue that it is very likely that due to the influence of privacy awareness, the users may feel they are in control of the information they submit on the SNSs that may be misused by other SNS members, hence the non-significance of the influence of privacy concerns on trust in SNS members. However, due to the fact that users cannot control how their personal/private information on the SNS is used by SNS providers, a significant negative influence of privacy concerns is observed on trust in SNS provider. This finding is consistent with the findings of work done by Chang, Liu, & Shen[68] who found that privacy concern has a significant negative influence on trust in using LinkedIn. Chang, Liu, & Shen [68] state that because LinkedIn members mostly share their job-related information for career reasons, and the information disclosure on the site may be private between job seekers and providers or among groups with similar career interests, trust is very important for users on the site. Chang, Liu, & Shen [68] also found out that for users of Facebook, there was a non-significant relationship between privacy concern and trust in using the site. Chang, Liu, & Shen [68] state that relationships built on Facebook are based primarily on close friendships and acquaintances, hence, there is a less perceived risk in submitting non-confidential or non-career oriented information.

This result may also explain why Ghanaian SNS users share a lot of personal content online.

Privacy invasion experience was found to have a significant negative effect on trust in SNS provider as well as trust in SNS members. This implies that SNS users in Ghana who have had prior privacy invasion experience(s) have less trust in SNSs as compared to those who have not had one. We argue that the finding in the current study is logical, and is also in line with work done by Mohamed & Hawa [57], as well as reviews made by Chen, Beaudoin, & Hong [55] and Young & Quan-Haase [56] who had similar findings. We should also expect that Ghanaian SNS users who have been victims of revenge pornography would share less personal content online.

Privacy-seeking behavior was found to have a significant positive effect on trust in the SNS provider as well as trust in the SNS members. This finding implies that SNS users in Ghana who adopt strategies to protect their privacy on SNSs are likely to trust the SNSs more since they are confident their strategies will shield them from privacy risk. This finding is consistent with work by Young & Quan-Haase [56] who reported that SNS users use several privacy protection schemes in order to lessen privacy risks while still allowing them to reveal enough information to link up with colleagues and friends on Facebook. However, Malik et al. [33] found a non-significant relationship between privacy-seeking behavior and trust in a study on photo sharing on Facebook. Malik et al. [33] stated that the non-significant relationship was due to the fact that trust became negligible as users identified privacy protection strategies that they were confident will prevent privacy violations. Malik et al. [33] further state that users who vigorously involve themselves in several privacy protection schemes feel more self-assured and, thus, reveal more information and content. We, therefore, conclude that privacy protection strategies have the likelihood of making trust negligible. At the same time, privacy protection strategies can build trust in the SNS since privacy protection strategies give users confidence and help prevent privacy violations.

In line with studies by Chang & Heo [5], Malik et al. [33], and Wu, Huang, Yen, & Popova [59], the current study showed that trust in SNS provider and SNS members have a significant positive effect on self-disclosure. This finding implies that the higher the levels of trust Ghanaian SNS users have in the SNS members and the SNS provider, the higher the likelihood of sharing their personal information. Previous literature also shows that trust is one of the most powerful factors that influence users' activity and readiness to give out information and content on Facebook [5]. We did not identify any study that showed a negative effect of trust on self-disclosure in the literature to enable us to do further comparative analysis. The amount of self-disclosure shown by SNS users in Ghana will thus be a reflection of the amount of trust they have in SNS service providers and other SNS members.

6 Conclusion

6.1 Theoretical Implications

This study has made contributions to growing body of literature on social media related issues [69-80]. Particularly, the current study has theoretical implications for the

study of privacy, trust, and self-disclosure in the area of social media and online social networking. Not much research has been done in the area of social media and online social networking involving the quantitative analyses of the relationships between privacy, trust, and self-disclosure constructs. The current study distinguishes itself from similar previous studies because those studies have treated Trust as a one-dimensional mediating variable, for instance, Zlatolas et al. [37], Malik et al. [33], and Wu, Huang, Yen, & Popova [59] (see Appendix A). The current study treats Trust as a two-dimensional mediating variable between privacy and self-disclosure. The results of the quantitative analysis of the privacy concern – trust path in the research model, that is, the significant negative effect on trust in SNS provider, but a non-significant effect on trust in SNS members, shows the multidimensional nature of the trust construct.

Practical Implications. The current study emphasizes the importance of privacy protection strategies in the use of SNSs. Most importantly, the ability of a user to adjust the privacy settings of the SNS and develop privacy protection strategies are key to the use of SNSs. It is therefore important for SNS providers to expose users to the need to adjust their privacy settings to suit their individual perceptions of risk. In our opinion, this may be better achieved if SNS providers mandatorily take users through a short tutorial on privacy settings immediately after sign-up, and also intermittently drop hints on privacy settings whilst users browse the sites.

In order to improve trust, SNS providers must assure users of the safety of their personal information during registration for service, especially from the activities of third parties. Both privacy policies and seals may help build users' trust and alleviate their privacy concern.

Also, SNS users must consciously make an effort to adjust their privacy settings to their preference to give them the needed confidence to share their personal information freely, and also have an interesting user experience.

Limitations and directions for further research. Although the current study produced some interesting results that validated some theories and past research, a few limitations must be considered. First, the respondents were selected from three universities in Ghana. This sample cannot represent all SNS users. Secondly, the study used a cross-sectional design, which may not capture changes in behavior over time. A longitudinal design should be considered in future studies. Because the setting of the current study limits us from generalizing to other cultural frameworks and advanced economies, the research model could be tested in those settings. Finally, subsequent studies could investigate the moderating role of gender and age on the relationships in the model.

References

1. Amichai-Hamburger, Y., Hayat, T.: Social Networking. Int. Encycl. Media

Eff. (2017)
2. Lenhart, A.: Teens, Social Media & Technology Overview. , Washington DC (2015)
3. Ignatius, E., Kokkonen, M.: Factors contributing to verbal self-disclosure. Nord. Psychol. 59, 362–391 (2007). doi:10.1027/1901-2276.59.4.362
4. Stutzman, F., Gross, R., Acquisti, A.: Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. J. Priv. Confidentiality. 4, 7–41 (2012). doi:10.1145/1958824.1958880
5. Chang, C.W., Heo, J.: Visiting theories that predict college students' self-disclosure on Facebook. Comput. Human Behav. 30, 79–86 (2014). doi:10.1016/j.chb.2013.07.059
6. Debatin, B., Lovejoy, J.P., Horn, A.-K., Hughes, B.N.: Facebook and online privacy: Attitudes, behaviors, and unintended consequences. J. Comput. Commun. 15, 83–108 (2009)
7. Huang, H.-Y., Chen, P.-L., Kuo, Y.-C.: Understanding the facilitators and inhibitors of individuals' social network site usage. Online Inf. Rev. 41, 85–101 (2017). doi:10.1108/OIR-10-2015-0319
8. Zhu, Y., Bao, Z.: The role of negative network externalities in SNS fatigue. Data Technol. Appl. DTA-09-2017-0063 (2018). doi:10.1108/DTA-09-2017-0063
9. Maier, C., Laumer, S., Eckhardt, A., Weitzel, T.: Giving too much social support : social overload on social networking sites. 1–18 (2014). doi:10.1057/ejis.2014.3
10. Feng, Y., Xie, W.: Author ' s personal copy Computers in Human Behavior Teens ' concern for privacy when using social networking sites : An analysis of socialization agents and relationships with privacy-protecting behaviors.
11. Ghafla.com: Social Media Apps Ghanaians Visit The Most, http://www.ghafla.com/gh/social-media-apps-ghanaians-visit/
12. Chaffey, D.: Global social media research summary 2018, https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/
13. Salter, M., Crofts, T.: Responding to revenge porn: Challenges to online legal impunity. New views Pornogr. Sex. Polit. law. 233–256 (2015)
14. Petronio, S., Reierson, J.: Regulating the Privacy of Confidentialitv: Grasping the Complexities through Communication Privacy Management Theorv. In: Afifi, T.A. and Afifi, W.A. (eds.) Uncertainty, Information Management, and Disclosure Decisions: Theories and Applications. pp. 365–383. Routledge, New York (2009)
15. Frampton, B.D., Child, J.T.: Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. Comput. Human Behav. 29, (2013)
16. Petronio, S.: Boundaries of privacy: Dialects of disclosure. State University of New York Press., Albany, NY (2002)
17. Golish, T.D.: Stepfamily communication Strengths; Understanding the ties that bind. Hum. Commun. Res. 29, 41–80 (2003)

18. Special, W.P., Li-Barber, K..: Self-disclosure and student satisfaction with Facebook. Comput. Human Behav. 28, 624–630 (2012)
19. Yoon, S.J., Han, H.E.: Experiential approach to the determinants of online word-of-mouth behavior. J. Glob. Sch. Mark. Sci. 22, 218–234 (2012)
20. Qian, H., Scott, C.R.: Anonymity and self-disclosure on weblogs. J. Comput. Commun. 12, (2007)
21. Barth, S., de Jong, M.D.T.: The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telemat. Informatics. 34, 1038–1058 (2017). doi:10.1016/j.tele.2017.04.013
22. Zhou, T.: The effect of network externality on mobile social network site continuance. Program. 49, 289–304 (2015). doi:10.1108/PROG-10-2014-0078
23. Myerscough, S., Lowe, B., Alpert, F.: Willingness to provide personal information online: the role of perceived privacy risk, privacy statements and brand strength. J. Website Promot. 2, 115–140 (2008)
24. Angst, C.M., Agarwal, R.: Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. MIS Q. 33, 339–370 (2009)
25. Bansal, G., Zahedi, F.M., Gefen, D.: The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis. Support Syst. 49, 138–150 (2010). doi:10.1016/j.dss.2010.01.010
26. Joseph Phelps, Glen Nowak, Ferrell, E.: Privacy Concerns and Consumer Willingness to Provide Personal Information. J. Public Policy Mark. 19, 27–41 (2000). doi:10.1509/jppm.19.1.27.16941
27. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. 17, 61–80 (2006). doi:10.1287/isre.l060.0080
28. Culnan, M., Bies, R.: Consumer Privacy: Balancing Economic and Justice Considerations. J. Soc. Issues. 59, 323–342 (2003). doi:10.1111/1540-4560.00067
29. Laufer, R., Wolfe, M.: Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. J. Soc. Issues. 33, 22–42 (1977). doi:10.1111/j.1540-4560.1977.tb01880.x
30. Culnan, M.J., Armstrong, P.K.: Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organ. Sci. 10, 104–115 (1999). doi:10.1287/orsc.10.1.104
31. Rachels, J.: Why privacy is important. Philos. Public Aff. 4, 323–333 (2003)
32. Jeong, Y., Kim, Y.: Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. Comput. Human Behav. 69, 302–310 (2017). doi:10.1016/j.chb.2016.12.042
33. Malik, A., Hiekkanen, K., Dhir, A., Nieminen, M.: Impact of privacy, trust and user activity on intentions to share Facebook photos. J. Information, Commun. Ethics Soc. 14, 364–382 (2016). doi:10.1108/JICES-06-2015-0022
34. Fox, J., Moreland, J.J.: The dark side of social networking sites: An

exploration of the relational and psychological stressors associated with Facebook use and affordances. Comput. Human Behav. 45, 168–176 (2015). doi:https://doi.org/10.1016/j.chb.2014.11.083

35. Awad, Krishnan: The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. MIS Q. 30, 13 (2006). doi:10.2307/25148715
36. Choi, B.C.F., Jiang, Z.J., Xiao, B., Kim, S.S.: Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. Inf. Syst. Res. 26, 675–694 (2015). doi:10.1287/isre.2015.0602
37. Hölbl, M., Zlatolas, L.N., Welzer, T., Heric, M.: Computers in Human Behavior Privacy antecedents for SNS self-disclosure : The case of Facebook. 45, 158–167 (2015). doi:10.1016/j.chb.2014.12.012
38. Lee, Y., Kwon, O.: Intimacy, familiarity and continuance intention: An extended expectation-confirmation model in web-based services. Electron. Commer. Res. Appl. 10, 342–357 (2011). doi:10.1016/j.elerap.2010.11.005
39. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model Of Organizational Trust. Acad. Manag. Rev. 20, 709–734 (1995). doi:10.5465/amr.1995.9508080335
40. Friedman, B., Khan Jr., P.H., Howe, D.C.: Trust Online. Commun. ACM. 43, 34–40 (2000). doi:10.1145/355112.355120
41. Han, S., Ma, E., Hong, D., Kim, E., Park, J., Lee, I., Kim, J.: The Effect of using SNS to interpersonal relation and quality of life: focused on the moderating role of communication capability. J. Inf. Syst. 22, 29–64 (2013)
42. Flanagin, A.J., Metzger, M.J.: Internet use in the contemporary media environment. Hum. Commun. Res. 27, 153–181 (2001). doi:10.1093/hcr/27.1.153
43. Osatuyi, B.: Information sharing on social media sites. Comput. Human Behav. 29, 2622–2631 (2013). doi:10.1016/j.chb.2013.07.001
44. Zhou, T., Li, H.: Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. Comput. Human Behav. 37, 283–289 (2014). doi:10.1016/j.chb.2014.05.008
45. Earp, J.B., Antón, A.I., Aiman-Smith, L., Stufflebeam, W.H.: Examining Internet privacy policies within the context of user privacy values. IEEE Trans. Eng. Manag. 52, 227–237 (2005). doi:10.1109/TEM.2005.844927
46. Eastlick, M.A., Lotz, S.L., Warrington, P.: Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. J. Bus. Res. 59, 877–886 (2006). doi:10.1016/j.jbusres.2006.02.006
47. Galanxhi, H., Nah, F.F.-H.: Privacy Issues in the Era of Ubiquitous Commerce. Electron. Mark. 16, 222–232 (2006). doi:10.1080/10196780600841894
48. Lwin, M.O., Wirtz, J., Stanaland, A.J.S.: The privacy dyad. Internet Res. 26, 919–941 (2016). doi:10.1108/IntR-05-2014-0134
49. Wu, K., Yan, S., Yen, D.C., Popova, I.: Computers in Human Behavior The

effect of online privacy policy on consumer privacy concern and trust. Comput. Human Behav. 28, 889–897 (2012). doi:10.1016/j.chb.2011.12.008
50. Zhang, Y., Fang, Y., Wei, K.K., Ramsey, E., McCole, P., Chen, H.: Repurchase intention in B2C e-commerce - A relationship quality perspective. Inf. Manag. 48, 192–200 (2011). doi:10.1016/j.im.2011.05.003
51. Lee, S., Kim, B.G.: The impact of qualities of social network service on the continuance usage intention. Manag. Decis. 55, 701–729 (2017). doi:10.1108/MD-10-2016-0731
52. Tan, X., Qin, L., Kim, Y., Hsu, J.: Impact of privacy concern in social networking web sites. Internet Res. 22, 211–233 (2012). doi:10.1108/10662241211214575
53. O'Bien, D., Torres, A.: Social Networking and Online Privacy: Facebook Users' Perceptions. Irish J. Manag. 63–98 (2012)
54. Proudfoot, J.G., Wilson, D., Valacich, J.S., Byrd, M.D.: Saving face on Facebook: privacy concerns, social benefits, and impression management. Behav. Inf. Technol. 37, (2018)
55. Chen, H., Beaudoin, C.E.: An empirical study of a social network site: Exploring the effects of social capital and information disclosure. Telemat. Informatics. 33, 432–435 (2016). doi:10.1016/j.tele.2015.09.001
56. Young, A.L., Quan-Haase, A.: Privacy protection strategies on Facebook: The Internet privacy paradox revisited. Information, Commun. Soc. 16, 479–500 (2013). doi:10.1080/1369118X.2013.777757
57. Mohamed, N., Hawa, I.: Computers in Human Behavior Information privacy concerns , antecedents and privacy measure use in social networking sites : Evidence from Malaysia. Comput. Human Behav. 28, 2366–2375 (2012). doi:10.1016/j.chb.2012.07.008
58. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science (80-.). 347, 509–514 (2015). doi:10.1126/science.aaa1465
59. Wu, K.W., Huang, S.Y., Yen, D.C., Popova, I.: The effect of online privacy policy on consumer privacy concern and trust. Comput. Human Behav. 28, 889–897 (2012). doi:10.1016/j.chb.2011.12.008
60. Straub, D., Boudreau, M.-C., Gefen, D.: Validation guidelines for IS positivist research. Commun. Assoc. Inf. Syst. 13, 63 (2004)
61. Cheung, C., Lee, Z.W.Y., Chan, T.K.H.: Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. Internet Res. 25, 279–299 (2015). doi:10.1108/IntR-09-2013-0192
62. Henseler, J., Ringle, C.M., Sinkovics, R.: The use of partial least squares path modeling in international marketing. Adv. Int. Mark. 20, 277–319 (2009). doi:10.1108/S1474-7979(2009)0000020014
63. Henseler, J., Hubona, G., Ray, P.A.: Using PLS path modeling in new technology research : updated guidelines. (2016). doi:10.1108/IMDS-09-2015-0382
64. Fornell, C., Larcker, D.F.: Structural equation models with unobservable variables and measurement error: Algebra and statistics. J. Mark. Res. 382–

388 (1981)
65. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. 43, 115–135 (2014). doi:10.1007/s11747-014-0403-8
66. Hu, L., Bentler, P.M.: Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Struct. Equ. Model. a Multidiscip. J. 6, 1–55 (1999)
67. Hoadley, C.M., Xu, H., Lee, J.J., Rosson, M.B.: Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. Electron. Commer. Res. Appl. 9, 50–60 (2010). doi:10.1016/j.elerap.2009.05.001
68. Chang, S.E., Liu, A.Y., Shen, W.C.: User trust in social networking services: A comparison of Facebook and LinkedIn. Comput. Human Behav. 69, 207–217 (2017). doi:10.1016/j.chb.2016.12.013
69. Kapoor, KK, Tamilmani, K, Rana, NP, Patil, P, Dwivedi, YK and Nerur, S (2018). Advances in Social Media Research: Past, Present and Future. Information Systems Frontiers. 20(3), 531–558.
70. Aladwani, A. M., & Dwivedi, Y. K. (2018). Towards a theory of SocioCitizenry: Quality anticipation, trust configuration, and approved adaptation of governmental social media. International Journal of Information Management, 43, 261-272.
71. Hossain, M. A., Dwivedi, Y. K., Chan, C., Standing, C., & Olanrewaju, A. S. (2018). Sharing political content in online social media: A planned and unplanned behaviour approach. Information Systems Frontiers, 20(3), 485-501.
72. Shiau W-L, Dwivedi YK & Yang H-S (2017). Co-citation and cluster analyses of extant literature on social networks. International Journal of Information Management, 37(5), 390–399.
73. Shiau, W-L, Dwivedi, YK & Lai H-H (2018). Examining the core knowledge on Facebook. International Journal of Information Management, 43, 52-63.
74. Alalwan, A. A., Rana, N. P., Dwivedi, Y. K., & Algharabat, R. (2017). Social media in marketing: A review and analysis of the existing literature. Telematics and Informatics, 34(7), 1177-1190.
75. Dwivedi, Y. K., Kapoor, K. K., & Chen, H. (2015). Social media marketing and advertising. The Marketing Review, 15(3), 289-309.
76. Rathore, A. K., Ilavarasan, P. V., & Dwivedi, Y. K. (2016). Social media content and product co-creation: an emerging paradigm. Journal of Enterprise Information Management, 29(1), 7-18.
77. Shareef, M. A., Mukerji, B., Dwivedi, Y. K., Rana, N. P., & Islam, R. (2019). Social media marketing: Comparative effect of advertisement sources. Journal of Retailing and Consumer Services, 46, 58-69.
78. Abed, S. S., Dwivedi, Y. K., & Williams, M. D. (2015). Social media as a bridge to e-commerce adoption in SMEs: A systematic literature review. The Marketing Review, 15(1), 39-57.
79. Plume, C. J., Dwivedi, Y. K., & Slade, E. L. (2016). Social media in the market-

ing context: A state of the art analysis and future directions. Chandos Publishing.
80. Dwivedi, Y. K., Mäntymäki, M., Ravishankar, M. N., Janssen, M., Clement, M., Slade, E. L., ... & Simintiras, A. C. (Eds.). (2016). Social Media: The Good, the Bad, and the Ugly: 15th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2016, Swansea, UK, September 13–15, 2016, Proceedings (Vol. 9844). Springer.

Appendix A

Summary of models on privacy and self-disclosure

Independent variables	Mediator variables	Dependent variables	Reference
Privacy awareness Privacy-seeking behavior Privacy concerns	Trust Activity	Sharing intentions	Malik et al. (2016)
Privacy awareness Privacy social norms Privacy policy Privacy control	Privacy value Privacy concerns	Self-disclosure	Zlatolas et al. (2015)
Privacy Policy Online privacy concern	Trust	Willingness to provide personal information	Wu et al. (2012)

Appendix B

Research Items

Self-disclosure on SNS

SD1 I have a comprehensive profile on my favorite social networking site

SD2 I find time to keep my profile up-to-date

SD3 I keep my friends updated about what is going on in my life through my favorite social networking site

SD4 When I have something to say, I like to share it on my favorite social networking site

Trust in SNS's service provider

TP1 My favorite social networking site is open and receptive to the needs of its members

TP2 My favorite social networking site makes good-faith efforts to address most member concerns TP3 My favorite social networking site is also interested in the well-being of its members, not just its own

TP4 My favorite social networking site is honest in its dealings with me

TP5 My favorite social networking site keeps its commitments to its members

TP6 My favorite social networking site is trustworthy

Trust in SNS's members

TM1 Other members on my favorite social networking site will do their best to help me
TM2 Members on my favorite social networking site care about the well-being of other member on the site
TM3 Members on my favorite social networking site are open and receptive to each other's needs TM4 Members on my favorite social networking site are honest in dealing with each other
TM5 Members on my favorite social networking site keep their promises
TM6 Other members on my favorite social networking site are trustworthy

Privacy Invasion Experience

PIE1: I have you personally been victim of what felt like an invasion of privacy on a social networking site?
PIE2: I have heard or read during the last year about the use and potential misuse of personal information about users on social networking sites?

Privacy awareness

PA1: I have read the privacy statement of my favorite social networking site
PA2: The privacy statement of my favorite social networking site is easy to understand
PA3: The privacy settings of my favorite social networking site are easy to use
PA4: I understand all the privacy setting of my favorite social networking site
PA5: I am aware of all the appropriate actions to ensure my privacy on favorite social networking site
PA6: I am aware of my privacy rights and responsibilities on my favorite social networking site

Privacy-seeking behavior

PSB1: Since joining this social networking site, I have changed the privacy settings multiple times PSB2: I usually keep track of my photos shared on this social networking site
PSB3: I usually delete my photos shared on this social networking site
PSB4: I usually think carefully before sharing my photos on this social networking site

Privacy concerns

PC1: The information is share could be misused by the social networking site
PC2: The information I share on social networking sites could be accessed by third parties
PC3: The information I share on social networking sites could be misused by other use on the social networking site
PC4: The information I share on social networking sites could be seen by unwanted people
PC5: The information I share on social networking sites could reveal private information
PC6: Information I disclose on favorite social networking site could have negative consequences that I cannot foresee