



GOMAL UNIVERSITY JOURNAL OF RESEARCH



Gomal University, Dera Ismail Khan, Khyber Pakhtunkhwa, Pakistan

ISSN:1019- 8180 (Print)


ISSN: 2708- 1737 (Online)

Website	www.gujr.com.pk	HEC Recognized	Social Sciences	CrossRef	DOI:10.51380
---------	--	----------------	-----------------	----------	--------------

THE VALIDATION OF CONCERNS FOR INFORMATION PRIVACY (CFIP) SCALE FOR SOCIAL NETWORKING SITES

Amna Farzand Ali, Syeda Hina Batool & Khalid Mahmood

Institute of Information Management, University of the Punjab, Lahore, Pakistan

KEYWORDS	ABSTRACT
Social Networking Sites, Information Privacy Concerns, Exploratory Factor Analysis (EFA)	<p>This study aims to evaluate and validate information privacy concerns scale for social networking sites. Current study identifies seven significant factors through Exploratory Factor Analysis (EFA) which may work antecedents of information privacy concerns. Thus, in order to create a list of items for the measurement of instrument constructs, an extensive research of relevant literature was carried out. Later, the selected items were discussed with supervisors & sent to six information professionals for content validity. Pilot instrument based on literature was empirically validated by collecting the data from one hundred undergraduate students from selected universities. Exploratory factor analysis was used to confirm that the scale's construct validity. Furthermore, for internal reliability of the scale Cronbach's alpha coefficient was checked, the psychometric features of the 57-item measure were assessed with a group of 500 undergraduate students. Subsequently, valid & reliable 57-item Information Privacy Concerns Scale was validated, which could be tested and utilized to evaluate social networking users' information privacy concerns. This validated scale can be used in different contexts and among variant population groups to confirm its validity in the different settings.</p>  <p>© 2023 Gomal University Journal of Research</p>
Article History Date of Submission: 18-07-2023 Date of Acceptance: 22-09-2023 Date of Publication: 30-09-2023	
Corresponding Author	Amna Farzand Ali: amna.farzand@gmail.com
DOI	https://doi.org/10.51380/gujr-39-03-08

INTRODUCTION

Information and Communication Technology (ICT's) tools generally required to disclosure of private information by the users. A vast amount of personal information is gathered through Social Networking Sites (SNSs) and websites (online banking, online gaming, online shopping etc.). The intentional disclosure behaviors include sharing an opinion, posting private pictures, or expressing emotions over the SNSs applications. On other hand, lot of disclosures take place unexpectedly or without anyone's knowledge, like when someone browses without knowingly accepting cookies or disclosing personal information that third parties may use against them (Alashoor, 2019). Social networking sites keep vast volume of data about its user' personal and

social information. These media applications retain huge risk of privacy invasion/information exploitation as their algorithms not only use one's personal information for their own use, but they also provide it to others for diverse purposes in the diverse situation. These data gathering practices and manipulation of data by SNSs platforms are rising information privacy concerns in the users (Mutimukwe, Viberg, Oberg & Pargman, 2022; Mutambik, Lee, Almuqrin, Zhang & Homadi, 2023). Today's communication patterns are bringing tremendous changes in people's everyday life. Now people are more interested to use SNSs platforms due to their user-centered interfaces.

These user-centered interfaces motivate SNSs users' e to use these apps or to reveal more and more personal information about themselves. The shared personal information over the SNSs can be permanently stored and easily searched without user's consent (Debatin, Lovejoy, Horn, & Hughes, 2009). People's personal information serves as the price for these social networking platforms, which are not free. The privacy calculus approach proposes two major constructs; the perceived privacy risks that are examined by perceived benefits and privacy concerns that are measured by the SNSs content (Child, Haridakis, & Petronio, 2012; and Smith, Dinev, & Xu, 2011). Users may develop social networks and exchange an increasing amount of information on all SNSs platforms, including Facebook, Twitter, Instagram, LinkedIn, Snapchat etc. These easy to access and sharing features are raising privacy concerns. The risks of stalking, identity theft and cyber-bullying are growing with the advancement of technology. The interesting thing is that these privacy concerns do not restrict the use of SNSs platforms and the revelation of the personal information by the SNSs users. This disconnection of information privacy concerns and self-disclosure is called "Privacy Paradox" (Bélanger & Crossler, 2011; Dinev, McConnell, & Smith, 2015; Heravi et al., 2018; Smith et al., 2011; Wang, Sun, Dai, Zhang, & Hu., 2019; Groß, 2021).

The nature of information privacy research is interdisciplinary. Basically, information privacy & privacy are two different constructs but interchangeably used in information privacy concerns research. Smith et al. (2011) classified approaches towards general privacy into value based and cognate-based categories. According to value based approach, "general privacy" is basic human right that is part of society's system of social and moral values. On other hand, cognate based approach explains 'information privacy' as a basic right of any individual, institution, or group to decide the criterion for themselves at what time, in what way and which kind of information to share about them with others (Gross & Acquisti, 2005). This study uses privacy as a cognate-based approach. Few social media users have understanding that SNSs applications store their basic personal information. Whereas, they do not have idea at which level these companies can capture or use the provided private information for different commercial purposes (Mourey & Waldman, 2020). In this connection, this phenomenon raises questions of the privacy concerns among social networking sites users. Consequently, the privacy concerns can be originated from different sources such as peer behaviors or organizational practices. For instance, without the other person's permission, the social media user may publicly post personal information about them.

In same way, organizations share private information of SNSs applications with third parties. These SNSs tools follow the pattern of co-ownership which leads to enhance uncertainty and loss of control over the privacy (Sun et al., 2019). Alashoor, Han, and Joseph (2017) define that the privacy concerns are the level of degree to which a social media user is worried about SNSs users and providers practices affecting the handling of their private information regarding

collection, errors, secondary and improper use and control over the provided information. The value of the various data has been greatly increased by technological developments. This scale measures general concerns related to online privacy. It may not be specific to social networking sites, but it can be adapted for such purposes. These media applications retain the huge risk of privacy invasion or information exploitation as their algorithms not only use one's personal information for their own use, but they also provide it to others. Paul, Scheibe, and Nilakanta (2020) revealed that after 2016 the data of internet has been increased rapidly and therefore, approximately half of the data is generated through the Internet of Things (IoT) and mobile devices. Due to weak security protocols these electronic devices have become source of security leakage.

Problem Statement

In this information technology era, use of technological applications for the sake of information communication and sharing is growing rapidly. Wide variety of Social Networking Sites (SNSs) are available which give ease to use instant messaging and information sharing platforms for connecting, resource sharing, social communication. It is fact that most of SNSs applications work like a double-edge sword that not only provide promising possibilities for communication and interaction beyond geographical locations but also, they retain the risk of privacy invasion and personal information sharing with third parties (Grant & Osanloo, 2014). Due to this issue, the information privacy concerns are prevailing among the SNSs users. In information privacy, researchers are using two dominated (Kusyanti et al., 2017) scales such as 1: the Concerns for Information Privacy (CFIP) by Smith et al. (1996) 2: the Internet users' information privacy concerns (IUIPC) Malhotra et al., (2004). The focus of CFIP is on measuring the organizational information privacy concern, while IUIPC is based on CFIP but it shifts focus toward perception of internet user in context of the online companies' fairness and justice related to information privacy.

These scales measure information privacy in context of internet related privacy issues, however, scales evaluating information privacy concerns with the focus of SNSs applications are limited. While examining information privacy concerns of SNSs user usually researchers take items from diverse dispositional scales and combine them with these two dominated scales to examine the privacy related issues (Brady, Truxillo, Bauer, & Jones, 2020). This study aims to evaluate and validate Concerns for Information Privacy (CFIP) scale with its four dimensions (the collection, error, improper access and unauthorized secondary use) can be used as the valuable scale, while investigating information privacy concerns of Pakistani undergraduate Facebook users. Firstly, this scale was developed in U.S to assess individuals' concern about the organizational privacy practices, however, this study intends to test the contextual validity of CFIP scale. The review of literature suggests that different studies used different theories with APCO model to examine information privacy concerns but none of the study used social capital theory. This study also aims to bridge this gap in literature. Therefore, the development of an appropriate instrument in this regard will highlight significant factors and will be a valuable addition into literature of information privacy concerns research in information management. The research objective is accordingly:

1. To what extent the validity and reliability of CFIP scale can be confirmed with the APCO model.

LITERATURE REVIEW

Importance of SNSs & IPC

Approximately more than 4.48 billion people are using different SNSs platforms globally. The facebook with 2.96 billion monthly active users is largest and most well-known SNSs platform (Datareportal, 2023), which makes it world's number one and most visited website, other SNSs applications are such as Twitter, WhatsApp, Snapchat, Instagram, LinkedIn. Boyd and Ellison (2007) characterized SNSs as free web-based platforms that enable the users to create virtual presence profile, communicate in real time with family, friends, and share private information with others through the sharing of memories, stories, photos, and videos. Information privacy and privacy concerns related research have received a lot of interest in domains of Information Systems and Science (IS) as a result of the development of SNSs platforms and their use. It has become an interdisciplinary phenomenon because all the life domains are using different kinds of SNSs tools. Privacy is the biggest concern of all SNSs users particularly, Facebook users. Kirkpatrick (2010) highlighted according to Mark Zuckerberg, founder of Facebook that age of privacy is ended and is no longer social norm. This controversial statement raised many privacy concerns among the Facebook users, still, interestingly people still use it more than other SNSs applications.

Kokolakis (2017) stated that the people show contradictory behavior even though they retain privacy concerns or fear about the loss of control on their private information but still they share information, it is called "privacy paradox". Weinberger, Bouhnik, and Zhitomirsky-Geffet (2017) argued that SNSs user are aware of the privacy policies and information loss but they tend to share their particular information to gain advantages of social capital over networking. Researchers also focused on that psychological aspect 'who knows about you' play an important role in information disclosure while having privacy risks. Many researchers suggested that privacy calculus approach is the solution of this privacy paradoxical issue, because it offers cost and benefits at same time. As all SNSs users share their personal information to gain something (pleasure, entertainment, communication) by communicating with others from these platforms and loss control over the data is the cost which they pay in the form of privacy invasion by the platforms and users (Debatin et al., 2009; Dinev et al., 2015; Ellison, Steinfeld, & Lampe, 2007; Flender & Müller, 2012; Acquisti, Brandimarte, & Loewenstein, 2015; Alashoor et al., 2017; Benamati et al., 2017; Ozdemir et al., 2017; Heravi et al., 2018b; Zhang et al., 2022; Ying et al., 2023).

Scales Measuring IPC

Privacy risk has been defined as the level to which a group or an individual believe that possible loss of private information is associated with self-disclosure. On the same way, privacy benefits tend to measure the positive gains a group or an individual achieve from the personal release of information (Malhotra et al., 2004). The measurement of the privacy concerns is necessary in order to investigate privacy behaviors and outcomes that lead for the disclosure of the personal information over SNSs platforms. Smith et al. (1996) developed one of the earliest privacy concerns model based on the Concerns for Information privacy (CFIP) that includes (collection, error, improper access & unauthorized secondary use) constructs for organization information privacy concerns investigations. On other hand, Malhotra et al. (2004) offered internet User's Information Privacy Concern model having three dimensions (collection, control & awareness), both models are used and discussed in literature. Smith et al. (2011) proposed "Antecedents Privacy Concerns Outcomes (APCO)" macro model. This is high process model that informs

how privacy antecedents donate to information privacy concerns/leads to influence behavioral outcomes.

This is widely used model with integration of different theories, not only in information privacy research but also in online banking, e-marketing, e-health (Mutambik et al., 2023; Alashoor et al., 2017; Benamati et al., 2017; Ozdemir et al., 2017; Heravi et al., 2018b; Lankton & Tripp, 2013; Mohamed & Ahmad, 2012). A thorough examination of literature reveals that numerous studies have been carried out to investigate phenomena of concerns about information privacy. Various studies used different theories and models to explore, however, two scales (CFIP and IUICP) are popular among researchers. In this connection, the critical role of antecedents in information privacy concerns and outcomes investigated through different approaches and lenses of different theories. The previous research focused on the dependent and independent effect of information privacy concerns on outcomes. There is a lack of studies which examined the moderating role of information privacy concerns or use of CFIP scale for the individuals' perceptions regarding SNSs platforms investigation therefore, present study intends to fill this gap.

RESEARCH METHODOLOGY

Instrument Design

In the first phase of instrument development comprehensive review of related literature was done. Similar scales developed in the earlier studies were identified and possible items for the inclusion of scale development were selected. Thus, a list of 75 items based on constructs was generated. The initial choice of items was guided by the extant literature to formulate questions related to constructs then questions were selected and framed in such a way that directly can ask respondents to report their information privacy concerns or antecedents related levels. The questionnaire comprised of the total 75 items based on literature (Smith et al. 1996; Williams, 2006; Junglas et al., 2008; Hsu, 2014; Jin, 2016; Ersdal, & Skjærstad, 2016; Malik, Dhir, & Nieminen, 2016) data was gathered using 7-point Likert scale (1 strongly disagree to 7 strongly agree).

Content Validity

Content validity of questionnaire refers towards the relevance and representativeness of the questions content in questionnaire, usually judged by expert. This type of validity is required in which experts evaluate and read the content of the research instrument, which measures the constructs which truly researcher wants to measure (LoBiondo-Wood & Haber, 2013). For this purpose, six experts (two from computer science and four from library & information science) were selected who provided their opinion regarding diverse questions order, format, relevancy, language, clarity, design and duplication. One of the experts mentioned to avoid double-barrel questions and other suggest avoiding duplication of questions in privacy concerns construct. All suggestions were incorporated to prepare final version of questionnaire after discussing with both supervisors. Thus, the final questionnaire comprised the 57 items to investigate the phenomena.

Data Collection

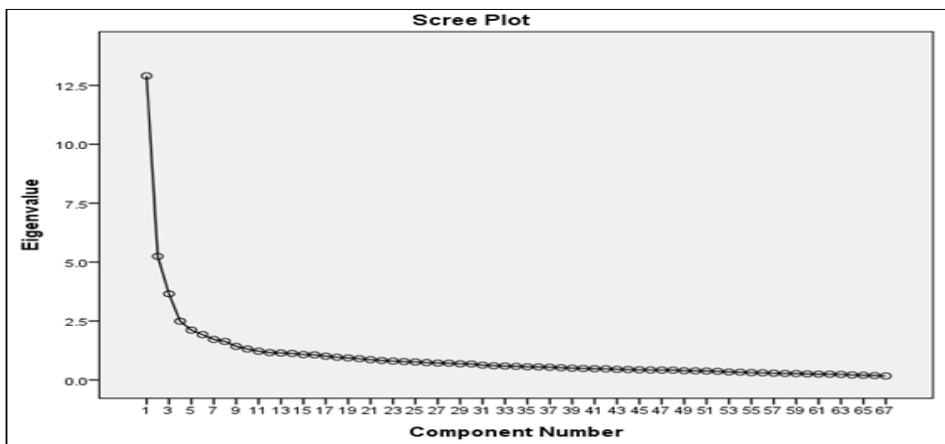
The final instrument was based on two portions; the first portion contained Social Networking Characteristics (use, intensity and diversity), and the other portion consisted of Antecedents (Awareness of Privacy Policy and Technology, Information Privacy Invasion and Social capital

bridging & bonding) → Privacy Concerns(Information Privacy Concerns) → Outcomes (Self-disclosure and Trust) (APCO) variables on a seven-point Likert type scale. Data were collected from undergraduate students regardless of discipline from top ten universities of Lahore (city). A comprehensive 405 usable responses which resulted 81% response rate. Exploratory Factor Analysis (EFA) was tested to assess validity of constructs. [Sekran and Bougie \(2016\)](#) mentioned that factor analysis is and appropriate method to measure the validity of constructs. It helps to recognize nature, number, merging factors of unlike sets, values, factor scores and hypothesis testing. To assess adequacy of sampling, Bartlett's Test of Sphericity and Kaiser-Meyer-Olkin (KMO) were utilized. These tests were significant (.05<.000), showing sampling method was appropriate (Table 2). Table 1 displays that KMO value is above (0.876) which point out sample acceptability and Barlett's test of Sphericity was (chi-square=11204.549, df= 2211, p<0.000) for seven factors shows items contained adequate common variance to apply EFA. According to [Kaiser \(1973\)](#), acceptable value of KMO is >0.50. Results of KMO value confirmed good sampling adequacy.

Table 1
KMO, Bartlett's Test of Sphericity

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.876
Bartlett's Test of Sphericity	Approx. Chi-Square	11204.549
	df	2211
	Sig.	.000
No. of Items		57

Figure 1
Scree plot Displaying Eigenvalues for Each Factor Component (405 respondents)



The rotation method helps to interpret the factors easily. Various rotation methods exist varimax rotation is one of them. [Mortelmans and Dehertogh \(2008\)](#) argued that varimax is helpful to retain good factors (subscales), it is important in this method to have factors which load >0.40. In this study, the Principal Component Analysis (PCA) with varimax rotation yielded 57 items and seven factors accounting for 51.473% of the total variance. Researchers suggested that total variance explained should be between 70% to 80%, however, in the social sciences extracted

factors explaining 50 % to 60% are thus acceptable (Institute of Digital Research & Education, 2020).

Factors Extraction

The rule of Kaiser (1970) is the foundation for factor extraction, which guides that components with the greater than 1.0 eigenvalues should be retained (variance amount between variable & component). If eigenvalue of factor is low, it means that factor has less contribution to explain the variance of variables. The scree plot examination helps in identification of factors in this regard Costello and Osborne (2005) mentioned that in scree plot look at natural break point or bend in data where curve like elbow occurs. In general, number of factors to keep is one above curve's break. Thus, number of elements above the "break" or elbow in the scree plot that were proposed to be extracted was seven, that was number that was considered to be most suitable in this case while investigating the scree plot elbow. The scree plot shows (Figure 1) that the eigenvalues start to form a straight line after the seven principal components for the present study.

Table 2

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	12.902	19.257	19.257	12.902	19.257	19.257
2	5.244	9.827	27.084	5.244	9.827	27.084
3	3.650	5.447	32.531	3.650	5.447	32.531
4	2.507	3.741	36.272	2.507	3.741	36.272
5	2.115	3.157	39.430	2.115	3.157	39.430
6	1.916	3.859	42.289	1.916	3.859	42.289
7	1.724	2.572	44.861	1.724	2.572	44.861

Table 3A

Total Variance Explained

Component	Initial Eigenvalues			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	12.902	19.257	19.257	6.844	10.215	10.215
2	5.244	9.827	27.084	4.977	9.428	17.643
3	3.650	5.447	32.531	4.156	6.203	23.846
4	2.507	3.741	36.272	3.991	5.957	29.804
5	2.115	3.157	39.430	3.746	5.591	35.394
6	1.916	3.859	42.289	3.083	4.587	47.583
7	1.724	2.572	44.861	3.074	3.700	51.282

Factors Labelling

Each item on the scale was labelled according to concepts that it was meant to cover in order to be used and analyzed for further study analysis. Thirteen items formed first factor, which had an eigenvalue= 12.902 and explained 10.215% of variation overall. Rotated factor loadings for elements in this factor range from 0.723 to 0.480. This factor was labelled 'Information Privacy Concerns'.

Table 4
Factor 1 Loadings for “Information Privacy Concerns”

SN	Items	Factor Loading
1	(33) Facebook should devote more time and effort to preventing unauthorized access to personal information.	0.723
2	(31) When people share personal information to Facebook for some reason, Facebook should never use the information for any other reason.	0.694
3	(34) Facebook should take more steps to make sure that unauthorized people cannot access personal information on their computer.	0.691
4	(30) Facebook should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.	0.689
5	(35) Facebook computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.	0.669
6	(29) Facebook should take more steps to make sure that the personal information in their files is accurate.	0.661
7	(32) Facebook should never sell the personal information in their computer databases to other websites or companies.	0.651
8	(26) All the personal information shared on the Facebook should be double-checked for accuracy.	0.633
9	(28) Facebook should devote more time and effort to verifying the accuracy of the personal information in their databases.	0.631
10	(27) Facebook should have better procedures to correct errors in personal information.	0.617
11	(24) When Facebook asks me for personal information, I sometimes think twice about providing it.	0.572
12	(23) It usually bothers me when Facebook asks me for personal information.	0.488
13	(25) I’m concerned that Facebook is collecting too much personal information about me.	0.480

Notes: N= 405, As an extraction technique, principal component analysis; as rotation technique, varimax on with Kaiser normalisation; Loading factors most significant loading inside factor

The second factor, titled "Self-Disclosure & Trust," had twelve items that explained 9.428% of the overall variance (eigenvalue = 5.244) (Table 4) and factor loadings ranging from (0.688 to 0.427).

Table 5
Factor 2 Loadings for “Self-Disclosure & Trust”

SN	Items	Factor Loading
1	(54) Facebook’s shared information is always true.	0.688
2	(53) People on Facebook are trustworthy.	0.649
3	(49) I often tell, personal things on my Facebook without hesitation.	0.643
4	(57) Security mechanism of Facebook is trustworthy.	0.636
5	(55) I trust Facebook unless it gives me a reason not to trust it.	0.601
6	(52) Overall, Facebook is trustworthy.	0.591
7	(47) I like my Facebook posts to be long and detailed.	0.577
8	(50) I share information on Facebook with people whom I don’t know in my day-to-day life.	0.570

9	(56) Facebook does respect and would not violate/misuse my privacy information and browsing log history.	0.545
10	(51) I frequently update my Facebook status/information.	0.531
11	(46) When I face challenges in my life, I feel comfortable talking about them with my Facebook friends.	0.427

Notes: N= 405, As an extraction technique, principal component analysis; as rotation technique, varimax on with Kaiser normalisation; Loading factors most significant loading inside factor

Third factor was identified as privacy management which contained ten items. These items had eigenvalue of 3.650 and explained 6.203% of total variance. In third factor the rotated factor loadings ranging 0.725 to 4.54 (Table 5).

Table 6
Factor 3 Loadings for "Privacy Management"

SN	Items	Factor Loading
1	(44) Deactivating or removing your profile.	0.725
2	(39) Editing or remove something you previously shared.	0.653
3	(45) Share the post with only me option.	0.648
4	(38) Deleting other's comments from your posts or pictures.	0.605
5	(43) Blocking people.	0.568
6	(42) Posting coded messages/inside jokes that only few of friends can know.	0.538
7	(41) Posting fake details like name, age, gender or location for sake of privacy.	0.534
8	(36) Removing friends from Facebook friend's list.	0.476
9	(37) Un-tagging yourself from the pictures to prevent revealing your identity.	0.455
10	(40) Configuring your profile to include location automatically on your posts.	0.454

Notes: N= 405, As extraction technique, principal component analysis; as rotation technique, varimax on with Kaiser normalization; Loading factors most significant loading inside factor

The fourth factor (eigenvalue= 2.407) exhibited 5.957 % of total variance and contained nine items. This factor was labeled as 'Social Capital Bonding' comprised items with rotated factor loadings between 0.678 to 0.404 (Table 6).

Table 7
Factor 4 Loadings for "Social Capital Bonding"

SN	Items	Factor Loading
1	(16) The people I interact with Facebook would put their reputation on the line for me.	0.678
2	(17) The people I interact with Facebook would be good job references for me.	0.635
3	(14) When I feel lonely, there are several people on Facebook I can talk to.	0.609
4	(15) 1 If I needed financial support, I know someone on Facebook who can help me.	0.598
5	(18) I do not know people on Facebook well enough to get them to do anything important.	0.566
6	(12) There is someone on Facebook, I can turn to for advice about making very important decisions.	0.536

7	(19) The people I interact on Facebook would persuade me to fight for an injustice.	0.519
8	(11) There are several people on Facebook, I trust to help solve my problems.	0.480
9	(13) There is no one on Facebook that I feel comfortable talking to about intimate personal problems	0.404

Notes: N= 405, As extraction technique, principal component analysis; as rotation technique, varimax on with Kaiser normalisation; Loading factors most significant loading inside factor

In fifth factor 5.601% of total variance was explained, contained four items with eigenvalue of 1.916. The items inside this factor ‘Awareness of Privacy Policy & Technology’ gained rotated factor loadings ranging from 0.706 to 0.642 (Table 7).

Table 7
Factor 5 Loadings for “Awareness of Privacy Policy & Technology”

SN	Items	Factor Loading
1	(3) I am technologically aware of how to customize/change Facebook privacy settings.	0.706
2	(1) I am aware of Facebook privacy policy statement.	0.680
3	(2) I can easily understand Facebook privacy policy statement.	0.680
4	(4) I can easily ensure my Facebook privacy settings.	0.642

Notes: N= 405, As an extraction technique, principal component analysis; as rotation technique, varimax on with Kaiser normalisation; Loading factors most significant loading inside factor

Six items were included in the sixth factor, which was categorized as ‘Social Capital Bridging’. The eigenvalue of these items was 1.724 and they clarified 4.587% of the overall variance. The items in the seventh factor ranging from 0.693 to 0.499 factor loadings (Table 9).

Table 8
Factor 6 Loading “Social Capital bridging”

SN	Items	Factor Loading
1	(8) Interacting with people on Facebook makes me feel like part of a larger community	0.693
2	(9) Interacting with people on Facebook reminds me that everyone in the world is connected.	0.587
3	(6) Interacting with people on Facebook makes me want to try new things.	0.580
4	(7) Interacting with people on Facebook makes me curious about what individual’s contrary to me think like.	0.568
5	(5) Interacting with people on Facebook makes me interested in things that happen outside of my town.	0.547
6	(10) Interacting with people on Facebook helps me talk to new people.	0.499

Notes: N= 405, As an extraction technique, principal component analysis; as rotation technique, varimax on with Kaiser normalisation; Loading factors most significant loading inside factor

The seventh factor was identified as ‘Privacy Invasion Experience’ which retained eigenvalue of 1.622 and accumulated for 3.700% of the overall variance. The rotated factor loadings for the items in this factor ranged from 0.665 to 0.486 (Table 9).

Table 9
Factor 7 Loadings for “Privacy Invasion Experience”

SN	Items	Factor Loading
1	(20) personally, experienced incidents whereby your personal information was used by someone without your authorization.	0.665
2	(21) personally, been the victim of what you felt was an improper invasion of privacy.	0.609
3	(22) heard or read during the last year about the use and potential misuse of consumer personal information without consumer authorization FB providers?	0.486

Notes: N= 405, As an extraction technique, principal component analysis; as rotation technique, varimax on with Kaiser normalisation; Loading factors most significant loading inside factor

Internal Consistency

In the next step, internal consistency of Likert type scale questions in questionnaire Cronbach’s Alpha (CA) was measured. The literature guides that, reliability of constructs should be at least 0.7. A moderate reliability should be between 0.7 and 0.9, whereas resilient reliability is greater than 0.9 (Houser, 2016). As result, it is assumed that tool is consistent. CA values (Table 10) show high level of internal consistency (reliability) of constructs. It reflects that developed scale is reliable.

Table 10
Internal Reliability of Scale

SN	Sub-scale	Number of items	Cronbach’s α
1	Information Privacy Concerns	13	.901
2	Self-Disclosure & Trust	12	.862
3	Privacy Management	10	.844
4	Social Capital Bridging	6	.801
5	Awareness of Privacy Policy & Technology	4	.816
6	Social Capital Bonding	9	.793
7	Privacy Invasion Experience	3	.677

DISCUSSION & CONCLUSION

The current study is quantitative in nature which assessed and validated a scale to measure the variables influencing information privacy concerns when using social networking sites, primarily Facebook, among undergraduate students. Total of 405 useable responses were used to survey the reliability and validity of 57-item final measure. This instrument was then experimentally examined. In order to check internal consistency Cronbach α coefficient was applied while EFA to validate instrument. Through EFA seven factors were extracted, notably it separated social capital bridging constructs items is factor four/social capital bonding construct items in factor seven. Interestingly, it also placed outcomes self-disclosure and trust items in the same factor two. Based on findings, current study has some crucial outcomes. As it introduces antecedent’s factors with combination of Social Capital (bridging & bonding) that affect information privacy concerns or in return affect outcome which are in line with previous research (Dinev, & Xu, 2011; Dinev, McConnell, & Smith, 2015; Heravi et al., 2018). The use of social capital theory in SNSs context with APCO model is a unique contribution. Use of CFIP scale in Pakistani context for investigating individual’s perceptions is a unique contribution because most of the previous

studies used it for organizations or in developed countries (Paul et al., 2020; Brady et al., 2020; Groß, 2021).

This study has used information privacy concerns as a moderating factor while previous had used it as mediating or antecedent (Alashoor et al., 2017; Sun et al., 2019; Mourey & Waldman, 2020). The present study is one of the unique exploratory studies to identify and organize the factors that contribute to information privacy concerns or in return affect outcomes. Moreover, this study added value to literature by validating a scale based on these factors. The empirical investigation also ensures strength of scale to be used in SNSs environment. Current research, like any other, has some limitations. Sample was based on undergraduate students only so it's findings cannot be generalized. Therefore, it is advised to investigate the perceptions of other population groups too. Data were collected from ten top universities of the one city of Pakistan however, sample size was appropriate to validate instrument. Another limitation is Exploratory Factor Analysis is a useful statistical tool for examining an instrument's construct validity and psychometric properties. However, since EFA is insufficient for testing instrument's theoretical foundations, a Confirmatory Factor Analysis (CFA) should be performed to advance knowledge in this field. Scale may also be refined further by using other theories with information privacy concerns.

REFERENCES

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.
- Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: APCO model. *Communications of the Association for Information Systems*, 41(1), 4.
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, 1017–1041.
- Benamati, H., Ozdemir, D., & Smith, H. J. (2017). An empirical test of an Antecedents - Privacy Concerns - Outcomes model. *Journal of Information Science*, 43(5), 583–600.
- Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-mediated Communication*, 13(1), 210–230.
- Brady, G. M., Truxillo, D. M., Cadiz, D. M., Rineer, J. R., Caughlin, D. E., & Bodner, T. (2020). Opening the black box: Examining the nomological network of work ability and its role in organizational research. *Journal of Applied Psychology*, 105(6), 637.
- Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: Variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, 28(5), 1859–1872.
- Costello, A. B., & Osborne, J. (2005). Best practices in exploratory factor analysis: Four recommendations for getting most from your analysis. *Practical Assessment, Research, and Evaluation*, 10(1), 7.
- Datareportal. (2023). global social media stats. <https://datareportal.com/social-media-users>.
- Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108.
- Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the “APCO” box. *Information Systems Research*, 26(4), 639–655.

- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends:” Social capital, college students’ use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143–1168.
- Ersdal, H. H., & Skjærstad, S. S. (2016). The Privacy and Social Media: Do Users Really Care?
- Flender, C., & Müller, G. (2012). Type indeterminacy in privacy decisions: the privacy paradox revisited. *International Symposium on Quantum Interaction*, 148–159.
- Grant, C., & Osanloo, A. (2014). Understanding, selecting, and integrating the theoretical framework in dissertation research: Creating the blue print for your house. December 2014.
- Groß, T. (2021). Validity and reliability of scale internet users’ information privacy concerns (iuipe). Proceedings on Privacy Enhancing Technologies.
- Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 71–80.
- Heravi, A., Mubarak, S., & Choo, K. R. (2018a). Information privacy in online social networks: Uses and gratification perspective. *Computers in Human Behavior*, 84, 441–459.
- Heravi, A., Mubarak, S., & Choo, K.-K. R. (2018b). The information privacy in online social networks: Uses and gratification perspective. *Computers in Human Behavior*, 84, 441–459.
- Houser, J. (2016). *Nursing Research: Reading, Using and Creating Evidence*. Jones & Bartlett Learning. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Houser%2C+J.+%282016%29.+Nursing+research%3A+Reading%2C+using+and+creating+evidence.+Jones+%26+Bartlett++Learning.&btnG=.
- Hsu, S. H. (2014). The Privacy paradox or bargained-for-exchange: capturing the relationships among privacy concerns, privacy management, self-disclosure, and social capital.
- Institute of Digital Research & Education. (2020). A Practical Introduction to Factor Analysis: Exploratory Factor Analysis. <https://stats.idre.ucla.edu/spss/seminars/introduction-to-factor-analysis/a-practical-introduction-to-factor-analysis/>.
- Jin, S. (2016). Understanding information privacy in the age of social media: cultural privacy boundary framework.
- Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4), 387–402.
- Kirkpatrick, M. (2010). Facebook’s Zuckerberg says the age of privacy is over. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134.
- Kusyanti, A., Puspitasari, R., Puspa, H., Catherina, A., April, Y., & Sari, L. (2017). Information Privacy Concerns on Teens as Facebook Users in Indonesia. *Procedia Computer Science*, 124, 632–638. <https://doi.org/10.1016/j.procs.2017.12.199>.
- Lankton, N. K., & Tripp, J. F. (2013). A quantitative and qualitative study of Facebook privacy using the antecedent-privacy concern-outcome macro model.
- LoBiondo-Wood, G., & Haber, J. (2013). Methods and critical appraisal for evidence-based practice. *Nursing Research: Text and Study Guide Package*, 290.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users’ information privacy concerns (IUIPC): the construct, the scale, and a causal model.
- Malik, A., Dhir, A., & Nieminen, M. (2016). Uses and gratifications of digital photo sharing on Facebook. *Telematics and Informatics*, 33(1), 129–138.

- Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366–2375.
- Mortelmans, D., & Dehertogh, B. (2008). Factoranalysis. Acco.
- Mourey, J. A., & Waldman, A. E. (2020). Past the privacy paradox: The importance of privacy changes as function of control and complexity. *Journal of the Association for Consumer Research*, 5(2), 162–180.
- Mutumukwe, C., Viberg, O., Oberg, L. M., & Pargman, T. (2022). Students' privacy concerns in learning analytics: Model development. *British Journal of Educational Technology*, 53(4), 932–951.
- Mutambik, I., Lee, J., Almuqrin, A., Zhang, J. Z., & Homadi, A. (2023). The Growth of Social Commerce: How It Is Affected by Users' Privacy Concerns. *Journal of Theoretical and Applied Electronic Commerce Research*, 18(1), 725-743.
- Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, 26(6), 642–660.
- Paul, C., Scheibe, K., & Nilakanta, S. (2020). Privacy concerns regarding wearable IoT devices: how it is influenced by GDPR? Proceedings of the 53rd Hawaii International Conference on System Sciences.
- Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. John Wiley & Sons.
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 989–1015.
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196.
- Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability*, 11(12), 3311.
- Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology & People*.
- Weinberger, M., Bouhnik, D., & Zhitomirsky, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science*, 1(1), 3–20.
- Williams, D. (2006). On and off the Net: Scales for social capital in an online era. *Journal of Computer-Mediated Communication*, 11(2), 593–628.
- Zhang, N. A., Wang, C. A., Karahanna, E. E., & Xu, Y. (2022). The Peer privacy concern: conceptualization and measurement. *MIS Quarterly*, 46(1).