

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/322533510>

# Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks

Article in *Journal of Global Marketing* · January 2018

DOI: 10.1080/08911762.2017.1412552

CITATIONS

59

READS

2,065

2 authors:



**Kishalay Adhikari**

International Management Institute

10 PUBLICATIONS 110 CITATIONS

[SEE PROFILE](#)



**Rajeev Kumar Panda**

National Institute of Technology Rourkela

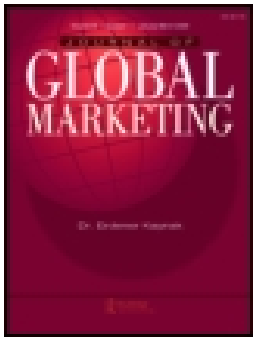
42 PUBLICATIONS 530 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Mediation analysis using SEM [View project](#)



# Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks

Kishalay Adhikari & Rajeev Kumar Panda

To cite this article: Kishalay Adhikari & Rajeev Kumar Panda (2018): Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks, Journal of Global Marketing, DOI: [10.1080/08911762.2017.1412552](https://doi.org/10.1080/08911762.2017.1412552)

To link to this article: <https://doi.org/10.1080/08911762.2017.1412552>



Published online: 16 Jan 2018.



Submit your article to this journal [↗](#)



Article views: 4




View related articles [↗](#)



View Crossmark data [↗](#)



## Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks

Kishalay Adhikari  and Rajeev Kumar Panda

School of Management, National Institute of Technology, Rourkela, Odisha, India

### ABSTRACT

The immense popularity of social networks has overshadowed the potential concerns, especially related to information privacy. Despite huge debates among privacy experts in recent times, seminal works have explored information privacy concerns from the perspective of social network users. In response, this research aims to understand the impact of antecedents of users' information privacy concerns (UIPC) on privacy protection behavior (PPB) in social networks. Drawing from the Social Cognitive Theory and Protection Motivation Theory, the research model was analyzed using structural equation modeling. The empirical results show that perceived vulnerability, perceived severity, and self-efficacy significantly influences UIPC. However, rewards and response efficacy did not significantly contribute towards UIPC. The linkage between UIPC and PPB was found to be statistically significant. This research article will offer newer insights for conceptual development and assist the social network's providers in redesigning their privacy protection strategies for safeguarding users from privacy threats.

### KEYWORDS

Information privacy concerns; privacy protection; protection motivation theory; social cognitive theory; social networks

### Introduction

The phenomenal growth of social networks (SNs) has taken the online world by storm; Facebook, Google Plus, and Twitter are the prominent examples. SNs fulfill the individual's desire for self-expression by enabling them to create a personal profile, develop connections, and interact with other users (Lim, Heinrichs, & Lim, 2017; Hudson et al., 2016; Basak & Calisir, 2015; Panek, Nardis, & Konrath, 2013; Chu & Choi, 2011; Sung et al., 2010). Across India, the SN penetration has touched the lives of over 136 million active users, the majority being college-going students (Statista, 2016). The SN giant Facebook has a staggering worldwide base of over 1.65 billion monthly active users. Also, 66% of Facebook users log into the site every day, while the average user spends one-fifth of their time online on Facebook, adding up to over 600 min/month on the website (Business Insider, 2015; VentureBeat, 2016).

The criticality of the issue of information privacy is reflected in the fact that 94% of Indians are concerned with their online privacy, as reported in research conducted by Big Brother Watch (2013) involving 10,354 online users from nine countries. During 2011–15,

more than a half million Indians were victims of privacy intrusions; i.e., their personal information was compromised (ASSOCHAM-Mahindra SSG report, 2015). In the global context, 48% of the respondents believed that personal medical information had been mishandled. Prior studies have investigated the sensitive issue of information privacy in healthcare, online commerce, and business transactional contexts (Dinev & Hart, 2004; Hong & Thong, 2013; Lee et al., 2007). However, less attention has been paid to exploring IP information privacy concerns with SN when users have control over the disclosure of personal information. Further, a majority of these studies have reported mixed findings regarding the antecedents of information privacy concerns. In developing a highly secured privacy system, it becomes vital for SN developers to clearly understand the predictors of information privacy concerns. Additionally, the users' responses to tackling information privacy concerns (i.e., protection behavior) would provide important insights for SN developers to redesign privacy mechanisms. To the best of our knowledge, seminal studies have investigated the linkage between information privacy concerns

and protection behavior in SN (Mohamad & Ahmed, 2012).

Based on the previously mentioned gap and ever-increasing social networking usage, the purpose of this research is to empirically validate the potent antecedents of users' information privacy concerns (UIPC) and to examine how UIPC influence privacy protection behavior (PPB) in the SN context. To suit the research, the authors have incorporated self-efficacy as an antecedent from Social Cognitive Theory. Similarly, Protection Motivation Theory was cited in the research to include the antecedents of perceived vulnerability, perceived severity, rewards, and response efficacy. Hence, the present study seeks appropriate answers to the following questions: (a) Do UIPC directly influence PPB in social networks? (b) What are the antecedents of UIPC in social networks? Both in academic and practical perspectives, this research seems of utmost relevance, as it contributes to the current understanding of information privacy, UIPC, and PPB by filling the knowledge gaps.

The remaining sections of this article adhere to the following sequence. In the initial section, the authors provide extant literature on user privacy concern and protection behavior in SN settings. The second section deals with the model development and formulation of associated hypotheses. The third section describes the analytic approach and discusses the findings of the tested hypotheses in the study. The concluding section talks about the theoretical, practical, and social implications of this study, points out the limitations, and highlights future research directions.

## Theoretical background

### *UIPC and PPB in social networks*

"User information privacy" can be defined as the "process of controlling the information boundary where individuals regulate the type, mode, and extent of personal information conveyed to others" (Lanier & Saini, 2008; Van De Garde-Perik et al., 2008). According to a body of research (Hong & Thong, 2013; Raschke, Krishen, & Kachroo, 2014; Belangar & Crossler, 2011; Xu et al., 2008), privacy is a dynamic, context-driven, and multidimensional construct, where Altman (1975) suggests that it encompasses interpersonal and social aspects and varies with life experience. User

information privacy refers to the user's ability to control information about himself or herself. Likewise, users' information privacy concerns (UIPC) deal with the degree of users' concern about the organizational practices of collection and use of their personal information (Smith, Milberg, & Burke, 1996). The association between privacy concerns and protection behavior was initially explored by Altman (1975, p. 50), suggesting that "People attempt to implement desired levels of privacy by using behavioral mechanisms. ..." Prior works in information systems research have found online privacy concerns significantly influence perceived trust and risk notions (Kansal, 2014; Smith, Dinev, & Xu, 2011; Malhotra, Kim, & Agarwal, 2004), as well as for protection behavior—the willingness to disclose online information (Son & Kim, 2008; Wang, Duong, & Chen, 2016). In an online environment, privacy concern is a vital ethical issue, since online companies are dependent on the collection and storage of users' personal information in their databases (Son & Kim, 2008; Young & Quan-Haase, 2013). This leads to an increase in users' concerns, since their personal information can be compromised by online companies (Feng & Xie, 2014; Shin, 2010). Moreover, users' responses to the privacy policy of Facebook were utilized to design a process model. The model precisely explained the initiation and outcome processes; i.e., emotive and behavioral aspects of UIPC (Burcu, Cavusoglu, & Benbasat, 2010). SNs offer exciting features to lure individuals to use them, yet social networks suffer from security threats, weak access controls, and feeble design (Acquisti & Gross, 2006). Once individuals become a part of SNs, they willingly disclose their personal information, such as present address, contact information, workplace details, etc. Although the SN may be equipped with privacy measures, it remains up to the user to activate them or use the default setting.

H1: There is a positive and significant linkage between UIPC and PPB in social networks.

### *Protection motivation theory*

Protection Motivation Theory (PMT) proposes that an individual's motivation to protect himself or herself from risks arises from three major components: perceived vulnerability, perceived severity, and response efficacy (Rogers, 1975). However, the earlier model

could not give sufficient explanations for individuals' failure to adopt a protective behavior. Subsequently, the model was modified and three cognitive constructs were included: self-efficacy, rewards, and response costs related to risky behavior (Maddux & Rogers, 1983; Rogers, 1975). According to Youn (2005, p. 90), PMT considers risks and benefits as crucial factors in explaining one's behavior in high-risk situations. Also, the motivation for self-protection enhances once individuals feel threatened by risky events (Boss et al., 2015; Mohamed & Ahmad, 2012; Youn, 2005). The theory finds its major application in health-related fields and is used to study behavior and intention (Searle et al., 2002; Milne, Orbell, & Sheeran, 2002; Lee et al., 2007a; Grindley, Zizzi, & Nasypany, 2008). Likewise, PMT offers insights regarding the influence of different behaviors in IS adoption (Woon, Tan, & Low, 2005; Pahlila, Sipponen & Mahmood, 2007; Milne, Labrecque, & Cromer, 2009). A major chunk of research related to PMT has focused on two prime areas—health studies and information systems research (Lee et al., 2007a; Lee, Lee, & Liu, 2007b). Empirical evidence for the use of PMT in the context of social networks, however, is not evident. Hence, based on its effective implementation in health studies and information systems research, we conceive that PMT can considerably explain UIPC and PPB in social networks. Unlike prior studies, wherein some variables of PMT, especially response costs and rewards, have been overlooked; this research considers all variables except response costs to provide a holistic view.

### **Perceived severity**

LaRose et al., (2005) refer to perceived severity as the conscious judgment of the severity outcomes resulting from a threatening security event. As such, a higher degree of perceived severity of the threat would compel online users' to adopt protection measures (Wang, Duong, & Chen, 2016; LaRose et al., 2005). Prior works have confirmed the vitality of perceived severity, showing that it significantly influences behavioral intention to use security features such as anti-spyware and wireless networks (Crossler, 2010, Chenoweth, Minch, & Gattiker, 2009). As far as teenagers are concerned, perceived risk and benefit appraisals explain a willingness to disclose personal information on SNs (Youn, 2005). In addition, there is empirical evidence that clearly

outlines the negative relationship between risk perceptions about information disclosure and willingness to render information (Youn, 2005). Zhang and McDowell (2009) have put forward an interesting insight wherein perceived severity does not motivate online users' to keep strong passwords. However, SN users who perceive information-privacy loss as a serious threat are more concerned about information privacy. Therefore, the current study proposes that there is a positive relationship between perceived severity and UIPC.

H2: Perceived severity positively and significantly influences UIPC in social networks.

### **Perceived vulnerability**

As delineated by Lee, LaRose, and Rifon (2008), Perceived vulnerability refers to the extent of users' belief that the threat might occur to them. Users' perception of perceived vulnerability regarding online virus threats will engage them in online protection behavior. Hence, a higher extent of vulnerability towards online viruses enhances the users' behavioral intention to take up online protection measures (Malhotra, Kim, & Agarwal, 2004; Lee, LaRose & Rifon, 2008) and the usage intention of anti-spyware (Liang & Xue, 2010; Chenoweth, Minch, & Gattiker, 2009). In this context, Dinev and Hart (2004) have found that perceived vulnerability positively affects online privacy concerns. In addition, consumers' view of negative consequences (online information leakage, frauds, identity theft, etc.) has positive linkage to privacy concerns (Crossler, 2010). Another critical aspect of perceived vulnerability concerns explains the reason behind data backup on computers and laptops (LaRose & Rifon, 2007). Thus, the current research posits that there is a positive relationship between perceived vulnerability and UIPC.

H3: Perceived vulnerability positively and significantly influences UIPC in social networks.

### **Response efficacy**

Woon, Tan, and Low (2005) refer to response efficacy as the individual's belief that a recommended coping response is effective in protecting the self or others from a threat. In connection with home wireless security, response efficacy has been found to be a

significant predictor of an individual's security measure use (Woon, Tan, & Low, 2005). Further, it critically explains the usage of anti-spyware to protect privacy (Chenoweth, Minch, & Gattiker, 2009), and affects users' intention to keep strong passwords (Zhang & McDowell, 2009) and retain data backups as a protective measure (Crossler, 2010). However, there is no direct association between response efficacy and adherence to information security policy (Zhang & McDowell, 2009). Therefore, users' who believe that negative consequences of losing information privacy can be tackled by protective action are more concerned about their information privacy. Hence, the study posits that there is a positive relationship between response efficacy and UIPC.

H4: Response efficacy positively and significantly influences UIPC in social networks.

### Rewards

Rewards pertain to expected benefits in connection with the behavioral choices (Mohamad & Ahmad, 2012). As noted by Youn (2009, p. 396), PMT (Rogers, 1975; Rogers, 1983) suggests, "perceived benefits associated with risky behaviors weaken intentions to self-protect from risks." In the same vein, users' participation in a social contract depends on higher perceived benefits that overbalance information-disclosure risks. Consequently, it reduces the motivation for privacy protection (Mohamed & Ahmad, 2012; Sheehan & Hoy, 2000). Due to their experiential nature, teens aged 13–19 are more vulnerable to disclosing personal information in SNs because of perceived benefits (Youn, 2005). In order to extract users' personal information (e.g., photos, email, contact details, etc.), SNs are using rewards (e.g., online games, apps, quizzes, etc.) as effective bait. Users who refrain from sharing this information are less prone to information privacy issues, virus attacks, and identity thefts. Contrary to this, users' who think otherwise and willingly share their information may gain more social acceptance from their peers (Baren et al., 2003). In addition, it enables them to fulfill the desire for self-expression and derive satisfaction by getting connected (Ijsselstein et al., 2009). Once the users' start experiencing the benefits of social connections, they may opt to share their personal information towards obtaining such benefits. Thus, the current study posits that there is a negative relationship between rewards and UIPC.

H5: Rewards negatively and significantly influence UIPC in social networks.

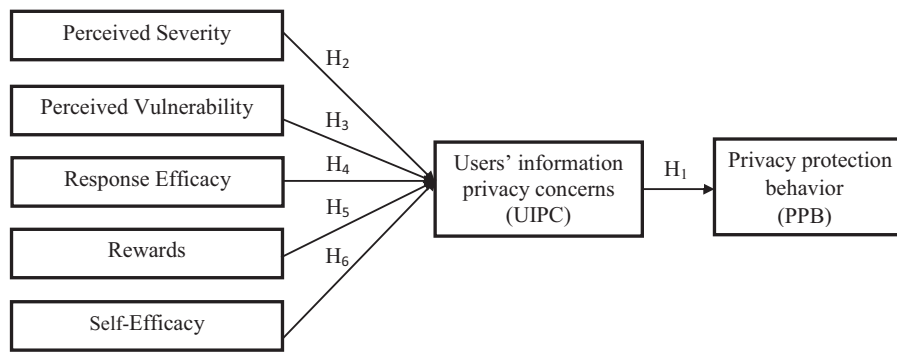
### Social cognitive theory

As stated by Bandura (1989), Social Cognitive Theory (SCT) is dynamic in nature and refers to the mutual interaction between the personal, behavioral, and environmental factors. The theory includes three vital relationships; the first one is between personal factors and behavior; i.e., based on individual beliefs, thought processes, and affective behavior (Bandura, 1986). The next relationship occurs among personal and environmental factors, wherein acquired experiences contribute to cognitive development. The interaction between environmental factors and behavior marks the third and final relationship. However, environmental factors are directly associated with individual behavior and their subsequent impacts. Thus, individual behavior is shaped by social rules and norms. Along the same lines, self-generated influences have a positive effect on behavior, whereas environmental factors significantly influence unhealthy practices (i.e., smoking, drug addiction, etc.). Hence, self-control plays a major role in predicting changes in such behavior. Consequently, self-efficacy can effectively determine social change (Bandura, 1995) and concerns with individual beliefs regarding the ability to carry out a particular behavior (Compeau, Higgins, & Huff, 1999).

### Self-efficacy

Over the last decade, self-efficacy has gained importance in information systems research studies. So far, the outcomes of extant self-efficacy studies in an online context are mainly equivocal. On the one hand, some scholars have found that self-efficacy has direct linkage with online privacy concerns (Awwal, 2011; Dienlin & Trepte, 2015); others have indicated otherwise (LaRose & Rifon, 2007). Along these lines, self-efficacy influences information privacy concerns (Korzaan & Boswell, 2008), impacts behavioral intention to adopt virus protection measures (Lee, LaRose & Rifon, 2008), and predicts protection behavior in online networks (Akhter, 2014; Chai et al., 2009; Milne, Labrecque, & Cromer, 2009). Further, self-efficacy positively affects user trust (Reid & Levy, 2008; Hsu et al., 2007), and contributes to preventive health behavior (Schwarzer





**Figure 1.** The hypothesized research model.

& Renner, 2000; Sheeran, Harris, & Epton, 2014; Prentince-Dunn & Rogers, 1986). In online spaces, consumers' confidence in their ability to tackle a risky event motivates them to secure their personal information (Cho, 2010; Milne, Labrecque, & Cromer, 2009).

However, other works involving self-efficacy have ascertained that it doesn't directly relate to information disclosure (Larose & Rifon, 2007) or privacy concerns (Youn, 2009). Nevertheless, self-efficacy has been investigated mainly with respect to intention to use online protection and virus protection measures; hence, there seems to be a gap in its application in SN privacy concerns. Accordingly, SN users who believe in their ability to protect their information will be concerned about privacy. As a result, they will adopt privacy protection behavior in SNs to minimize their privacy concerns. Hence, the research hypothesizes that there is a positive relationship between self-efficacy and UIPC (Figure 1).

H6: Self-efficacy positively and significantly influences UIPC in social networks

## Research methods

### Instrument development and subjects

The targeted samples were gathered from among university students at a major central university in India. The student population of the university is nearly 5000 and represents a culturally diversified group. Based on simple random sampling technique, the respondents were selected using random numbers from the university admission list. Also, two prime considerations regarding the samples were kept in mind; i.e., age-group of 18–34 years and having SN

profiles. Samples not adhering to the aforementioned criteria were eliminated at the outset. Sample size determination was conducted using a priori sample size calculator for SEM developed by Soper (2015). Based on the calculation of effect size and statistical power, the minimum sample size came to be around 210 samples. Therefore, we distributed 410 questionnaires (approximately twice the minimum sample size) to gather the required responses. The questionnaires were distributed over a three-week period in September 2016. Faculty members of various departments were approached to speed up the data collection process. Their voluntary participation helped us with distribution, filing, and collection of the questionnaires from the students. Both the students and faculty members were assured of the confidentiality of the accumulated information. The response rate was increased by weekly follow-ups with the faculty members. A total of 410 questionnaires were distributed, out of which 337 responses were received. A total of 306 responses were used for final analysis after discarding 31 incomplete and invalid responses. To check for non-response bias, we compared the early-filled questionnaires with the late-filled ones and discovered no significant differences between both groups. Hence, the respective sample does not suffer from non-response bias. Table 1 exhibits the demographic profile of the respondents.

### Measurement development

The measurement items of the constructs were drawn from extant literature, thereby ensuring adequate content validity. As per the final research instrument, UIPC were measured using a five-item scale wherein three items were adapted from Dinev and Hart (2004) and

**Table 1.** Demographic profile of the respondents.

<i>Demographic characteristics</i>	<i>Frequency (% of total)</i>
<i>Median age</i>	22
<i>Gender</i>	
Male	178 (58.17%)
Female	128 (41.83%)
<i>SN use duration</i>	
<1 year	19 (6.21%)
1–3 years	47 (15.36%)
3–5 years	148 (48.37%)
5+ years	92 (30.06%)
<i>Daily time spent on SN</i>	
Less than 30 mins	42 (13.72%)
30 mins to 1 hr	83 (27.12%)
1–2 hrs	124 (40.52%)
More than 2 hrs	57 (18.62%)

the other two items were self-developed. The adapted items of UIPC measure the users' concerns regarding inappropriate use and unauthorized access of their personal information in a SN. Self-developed items of UIPC include usually think twice before submitting my personal information in SNs and feel that SNs are collecting excessive personal information. Response efficacy was measured using three items adapted from Lee, Larose, and Rifon (2008), Zhang and McDowell (2009), and Crossler (2010). Self-efficacy was measured by three items adapted from Woon, Tan, and

Low (2005), Larose and Rifon (2007), and Crossler (2010). Perceived vulnerability was measured using three items adapted from Dinev and Hart (2004) and Woon, Tan, and Low (2005). Measurement items for perceived severity were adapted from Woon, Tan, and Low (2005) and Crossler (2010). Items for measuring rewards were based on prior scales used by Youn (2009). Finally, PPB was measured using six items adapted from past researchers (Sheehan & Hoy, 1999; Milne & Culnan, 2004; Youn, 2009; Krasnova et al., 2010). The items of PPB essentially measure refusal and misinterpretation of personal information to protect information privacy. The respondents rated each construct items on a 7-point Likert scale in which "1" signifies "Strongly Disagree" and "7" signifies "Strongly Agree." The mid-value of "4" indicates a neutral or uncertain response. To eliminate discrepancies in the structure of the questionnaire, pre-testing was conducted with seven doctoral scholars and two faculty members working in similar research domains. The legibility of the questionnaire was improved as necessary modifications were made based on the feedback. Table 2 shows the final questionnaire used in the study.

**Table 2.** Questionnaire items used in final analysis.

<i>Construct</i>	<i>Measurement items</i>
Perceived severity	PS1 Losing information privacy through social networks would pose serious problems for me. PS2 Online identity theft through social networks would create serious problems for me. PS3 Misuse of personal information available in social networks would pose serious problems for me. PS4 Losing photo privacy through social networks would pose serious problems for me.
Perceived vulnerability	PV1 I could potentially suffer from malicious online security issues (e.g., privacy intrusions, virus attacks, etc.) in social networks. PV2 I feel at risk when I share personal information in social networks. PV3 I feel it is not safe to share personal information in social networks.
Self-efficacy	SE1 I believe I possess the ability to safeguard my personal information in social networks. SE2 I believe I can enable the privacy protection features in social networks without any assistance. SE3 I am confident when using privacy protection features in social networks.
Response efficacy	RE1 Enabling privacy protection features in social networks could protect me from information privacy threats. RE2 If I use privacy protection features in social networks, I am less vulnerable to lose my information privacy. RE3 I can effectively control my information privacy using privacy protection features in social networks.
Rewards	REW1 By compromising my personal information in social networks, I could get in touch with old friends and make new connections. REW2 By compromising my personal information in social networks, I could participate in online games and applications. REW3 By compromising my personal information in social networks, I could become a member of social groups.
Users' information privacy concerns	UIPC1 I am concerned that my personal information in social networks could be used for wrong purposes. UIPC2 I am concerned that my personal information in social networks could be accessed by unknown parties. UIPC3 I usually think twice before providing my personal information in social networks. UIPC4 I feel social networks are collecting excessive personal information. UIPC5 I am concerned that my personal information in social networks could be used in a manner I am unaware of.
Privacy protection behavior	PPB1 I consciously misrepresent specific personal information in social networks. PPB2 I willfully provide incomplete personal information in social networks. PPB3 I deliberately provide false personal information in social networks. PPB4 I deliberately refrain from giving specific personal information in social networks. PPB5 I consciously avoid giving specific personal information in social networks. PPB6 I willingly refuse to provide specific personal information in social networks.



**Table 3.** Measurement model reliability.

Construct	Measurement item	Standardized loadings	Cronbach $\alpha$	CR	AVE
Perceived severity	PS1	0.756	0.840	0.841	0.571
	PS2	0.656			
	PS3	0.801			
	PS4	0.805			
Perceived vulnerability	PV1	0.749	0.860	0.861	0.675
	PV2	0.848			
	PV3	0.863			
	REW1	0.744			
Rewards	REW2	0.759	0.842	0.849	0.654
	REW3	0.913			
Response efficacy	RE1	0.717	0.781	0.783	0.547
	RE2	0.697			
	RE3	0.801			
	SE1	0.785			
Self-efficacy	SE2	0.879	0.883	0.885	0.721
	SE3	0.867			
	UIPC1	0.818			
	UIPC2	0.885			
Users' information privacy concerns	UIPC3	0.815	0.908	0.910	0.670
	UIPC4	0.847			
	UIPC5	0.720			
	PPB1	0.750			
Privacy protection behavior	PPB2	0.713	0.916	0.915	0.644
	PPB3	0.864			
	PPB4	0.845			
	PPB5	0.820			
	PBB6	0.811			

## Data analysis and results

We followed a two-step analytic approach (Anderson & Gerbing, 1988) for examining the construct validity and testing the proposed hypotheses using Structural Equation Modeling (SEM) in AMOS 20.0 software. Firstly, the measurement model was analyzed for ensuring construct validity, reliability, and goodness of fit. Secondly, we assessed the structural model for determining the model fit using multiple fit indices. As a rule of thumb, fit indices should include  $\chi^2$  value, df, and one index of absolute-fit, incremental-fit, goodness-of-fit, and badness-of-fit to ensure good model fit (Hair et al., 2010, p. 678).

### Measurement model validation

A seven-factor measurement model was developed to assess the reliability and validity of the research instrument under the confirmatory factor analysis (CFA) approach. Items were restricted in such a manner that they load only on a predefined construct. On the other hand, each construct was allowed to correlate freely among them. To assess construct reliability, Cronbach's  $\alpha$  and composite reliability (CR) were examined. Table 3 shows that Cronbach's  $\alpha$  of each construct

ranged between 0.781 and 0.916, greater than accepted values of 0.70 (Nunnally & Bernstein, 1994). As for the CR, the minimum value in our research model was 0.783, satisfying the recommended threshold of 0.70 (Fornell & Larcker, 1981). Hence, CR and Cronbach's  $\alpha$  value indicated that the constructs used in the research model were reliable (see Table 3).

Subsequent to the reliability check, construct validity was assessed using the criterion of convergent validity (CV) and discriminant validity (DV). According to Hair et al., (2012), CV can be assessed by determining whether each item's standardized loading on the corresponding construct is greater than 0.50 and statistically significant. Relationally, the standardized loadings exceeded the benchmark values ( $\geq 0.50$ ) and significance ( $p$ -value 0.01), thereby satisfying the criteria for CR. Further, the test of DV showed that the square root of the average variance extracted (AVE) of all the constructs was higher than the inter-construct correlations. Accordingly, these values affirmed that all of the construct measures in our research model achieved DV (see Table 4). The goodness-of-fit statistics for the measurement model indicated adequate model fit (CMIN = 492.217, df = 303, CMIN/df = 1.624, GFI = 0.896, AGFI = 0.87, CFI = 0.96, IFI = 0.961, NFI = 0.904, RMSEA = 0.045, RMR = 0.062). Thus, the model reflected construct

**Table 4.** Discriminant validity.

	Mean	S.D.	Perceived severity	Self-efficacy	Rewards	Perceived vulnerability	Response efficacy	Users' info. privacy concerns	Privacy Protection behavior
Perceived severity	5.833	1.051	0.755						
Self-efficacy	5.605	1.141	0.370	0.849					
Rewards	5.367	1.197	0.015	0.056	0.809				
Perceived vulnerability	5.580	0.982	0.409	0.450	0.098	0.822			
Response efficacy	4.679	1.753	0.126	0.168	0.037	0.038	0.739		
Users' info. privacy concerns	5.373	1.024	0.463	0.522	0.027	0.614	0.079	0.819	
Privacy protection behavior	5.841	0.925	0.294	0.503	0.194	0.490	0.121	0.551	0.802

(Note. The table indicates correlation values among constructs whereas diagonal values represent the square root estimate of AVE).

validity, goodness-of-fit, construct reliability, and suitable psychometric properties.

### Dealing with common method bias

The current study used a self-reported questionnaire to carry out data collection; however, the primary concern with survey scales is the presence of measurement error and common method variance. Most often, such error can lead to bias in estimating the relationship between the constructs.

### Harman's single-factor test

To assess CMB, we conducted Harman's single-factor test (Podsakoff et al., 2003). In the first place, entire items in the study were examined through an EFA procedure that included principal-component extraction, unrotated factor solution, and varimax rotation. The EFA results revealed seven factors; each of them has eigenvalues greater than 1.0. Also, there was no presence of a dominant factor as per the analysis. The cumulative variance explained by the seven factors was 74%, out of which the first factor accounted for 31.086% of the variance that fell below the 50% criterion recommended by Harman (1976). Recently, the prominent advantages of high accuracy and robustness have impelled researchers to execute Harman's single-factor test with confirmatory factor analysis (CFA) (Craighead et al., 2011; Mishra, Kesharwani, & Das, 2016). The robustness and accuracy of the CFA procedure can be observed from the fact that it provides model fit indices for the multi-factor and single-factor models, while highlighting the discrepancies between the respective models through a chi-square difference test. In cases where the model fit indices of the two models and their chi-square differences manifest that the multi-factor model is significantly better than the single-factor model across all parameters, we can

deduce that the data set doesn't suffer from CMB (Mishra, Kesharwani, & Das, 2016; Byrne, 2016).

Table 5 indicates that the measurement model is conforming to the recommended model fit indices, ensuring good model fit. The chi-square differences between the multi-factor and single-factor models are found to be significant; i.e., the multi-factor model is exhibiting best model fit as compared to the single-factor model. In addition, the other model-fit indices also exceeded the index difference threshold limit of 0.001 (Byrne, 2016).

### Unmeasured Latent Method Construct (ULMC)

The assessment of CMB using the ULMC procedure can be performed through two approaches. The first approach, advocated by Lindell and Whitney (2001), proposes creating a measurement model appended by a common latent factor (CLF) to which all indicators are loaded in addition to their theoretically related factor. Path coefficients from CLF to the respective measurement indicators were constrained to be equal, as it is conceived that the influence of CMB would be similar across all measurement indicators. The subsequent evaluation of both measurement models (with CLF and without CLF) evidenced the absence

**Table 5.** Common method bias assessment through Harman's single-factor test.

Model-fit indices	Multi-factor model	Single-factor model	Difference ( $\Delta$ )
CMIN	492.217	649.104	156.887
DF	303	321	18
CMIN/DF	1.624	2.022	0.398
CFI (Comparative fit index)	0.96	0.931	0.029
GFI (Goodness-of-fit index)	0.896	0.874	0.022
IFI (Incremental fit index)	0.904	0.873	0.031
NFI (Normed fit index)	0.961	0.932	0.029
RMR (Root mean square residual)	0.045	0.058	-0.013
RMSEA (Root mean square error of approximation)	0.062	0.590	-0.528

of CMB, as the models were significantly different. Model-fit statistics of the measurement model with CLF ( $\chi^2 = 455.182$ ,  $df = 297$ ,  $\chi^2/df = 1.533$ , CFI = 0.967, RMSEA = 0.051, RMR = 0.073) show a significant difference from the measurement model without CLF ( $\chi^2 = 492.217$ ,  $df = 303$ ,  $\chi^2/df = 1.624$ , CFI = 0.96, RMSEA = 0.045, RMR = 0.062). The estimation of chi-square difference ( $\Delta\chi^2$ ) showed 37.035 with 6 degrees of freedom; i.e.,  $\Delta\chi^2/\Delta df$  value = 6.1725, which exceeds the recommended cut-off criterion of 3, thereby exhibiting significant change in the model (Hair et al., 2012). Additionally,  $\Delta CFI = 0.007$ ,  $\Delta RMSEA = 0.006$ ,  $\Delta RMR = 0.011$  values are above the threshold limit of 0.001. Hence, the comparison of overall model fit indices and low path coefficients does not influence the measurement of the scale indicators.

In another approach, suggested by Byrne (2010), both measurement models (with and without CLF) were separately analyzed and their standardized path coefficients were noted (Table 6). The difference between the standardized path coefficients falls in the range of 0.001 to 0.178, implying that CLF explains maximum variance of 3.168% ( $0.178 \times 0.178 = 0.03168$ ) for any measurement item. Overall, the marginal differences in standardized path coefficients support the absence of CMB in the data set.

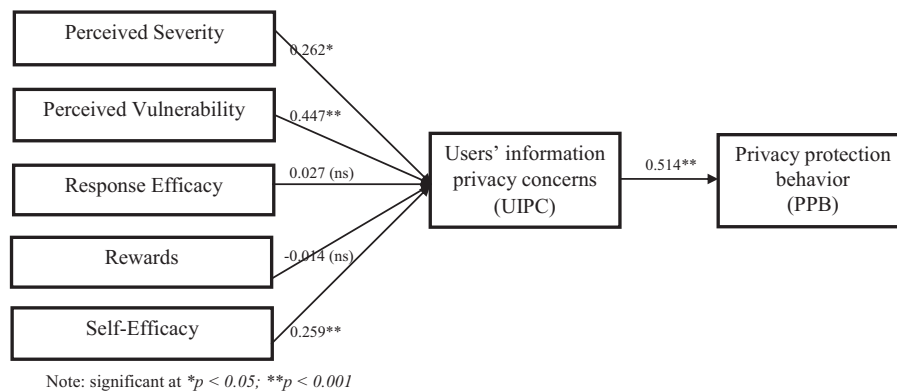
### Structural model estimation

The prime objectives of this study were to empirically validate the hypothesized model and assess the linkage between the potent antecedents, UIPC and PPB, in social networks in the Indian context. The constructs of perceived severity, response efficacy, self-efficacy, rewards, and perceived vulnerability contributed 52%

**Table 6.** Unmeasured latent construct method for common method bias estimation.

Measurement item	Standardized estimates (with CLF)	Standardized estimates (without CLF)	Change
PS1	0.750	0.756	0.006
PS2	0.647	0.656	0.009
PS3	0.781	0.804	0.023
PS4	0.796	0.805	0.009
PV1	0.730	0.749	0.019
PV2	0.772	0.848	0.076
PV3	0.815	0.863	0.048
REW1	0.743	0.744	0.001
REW2	0.748	0.759	0.011
REW3	0.905	0.913	0.008
RE1	0.713	0.717	0.004
RE2	0.683	0.697	0.014
RE3	0.792	0.801	0.009
SE1	0.650	0.785	0.135
SE2	0.701	0.879	0.178
SE3	0.786	0.867	0.081
UIPC1	0.776	0.818	0.042
UIPC2	0.796	0.885	0.089
UIPC3	0.696	0.815	0.119
UIPC4	0.762	0.847	0.085
UIPC5	0.667	0.720	0.053
PPB1	0.725	0.750	0.025
PPB2	0.633	0.713	0.080
PPB3	0.814	0.865	0.051
PPB4	0.743	0.845	0.102
PPB5	0.747	0.820	0.073
PPB6	0.758	0.811	0.053

( $R^2 = 0.52$ ) of the total variation in UIPC, whereas UIPC in turn explained 36% ( $R^2 = 0.36$ ) of the total variation in PPB (see Figure 2). The results in Table 7 show  $CMIN = 500.840$ ,  $df = 306$ ,  $CMIN/df = 1.637$ ,  $p$ -value = 0.000. However, various indicators, apart from  $CMIN$  and  $p$ -value, were also considered to ascertain good model fit. The indicators CFI, GFI, IFI, TLI, and NFI for the hypothesized model exceeded the commonly accepted values of 0.90, indicating an appropriate fit to the data. Also, the values of RMSEA = 0.046 and SRMR = 0.078 were lower than the recommended level of 0.08 suggested for the close fit of the model. In totality, the findings of the structural



**Figure 2.** Results of hypothesis testing.

**Table 7.** Model fit indices for measurement model and structural model.

Fit index	Recommended value	Measurement model	Structural model
CMIN/df (Chi-square; df)	$\leq 3$	1.624 (492.217; 303)	1.637 (500.840;306)
CFI	$\geq 0.90$	0.96	0.959
GFI	$\geq 0.80$	0.896	0.894
AGFI	$\geq 0.80$	0.870	0.869
NFI	$\geq 0.90$	0.904	0.902
IFI	$\geq 0.90$	0.961	0.960
RMSEA	$\leq 0.08$	0.045	0.046
RMR	$\leq 0.08$	0.062	0.078

model were satisfactory. The path's beta coefficient and level of significance ( $p$ -value) are shown in Table 8.

The results shown in Table 8 and Figure 2 indicate that most of the hypotheses are supported. First, the linkage between UIPC and PPB is found to be statistically significant ( $\beta = 0.514$ ,  $p < 0.001$ ), thus supporting H1. This result extended strong support to the prior studies (Son & Kim, 2008; Malhotra, Kim, & Agarwal, 2004; Korzaan & Boswell, 2008; Mohamed & Ahmad, 2012). Second, the effect of perceived severity on UIPC is significant and positive ( $\beta = 0.262$ ,  $p < 0.05$ ), in support of H2. This finding is in line with a majority of previous studies (Larose et al., 2005; Chenoweth, Minch, & Gattiker, 2009; Mohamed & Ahmad, 2012), while it differs from Zhang and McDowell (2009), thus highlighting the fact of mixed findings regarding perceived severity. Third, perceived vulnerability positively and significantly influences UIPC ( $\beta = 0.447$ ,  $p < 0.001$ ), thus supporting H3. Perceived vulnerability is evidenced to be a strong antecedent of UIPC, unlike previous work by Mohamed and Ahmad (2012). Moreover, this result lends considerable support to the findings of Dinev and Hart (2004) and Crossler (2010). Fourth, response efficacy has no significant impact on UIPC ( $\beta = 0.027$ ,  $p > 0.005$ ), thus rejecting H4. Our results did not support this relationship, thus contradicting the earlier studies (Sheehan & Hoy, 2000;

Phelps, Nowak, & Ferrell, 2000). Fifth, reward does not have any significant influence on UIPC ( $\beta = -0.014$ ,  $p > 0.005$ ), rejecting H5. Interestingly, this result contradicts the existing literature (Chenoweth, Minch, & Gattiker, 2009; Crossler, 2010; Zhang & McDowell, 2009). Lastly, self-efficacy has a significant influence on UIPC ( $\beta = 0.259$ ,  $p < 0.001$ ), thus affirming H6. Prior researchers have reported this relationship quite differently; some in agreement (Maddux & Rogers, 1983; Lee, Larose, & Rifon, 2008; Chai et al., 2009; Milne, Labrecque, & Cromer, 2009) and others who disagreed (Larose & Rifon, 2007; Youn, 2009).

## Discussion and conclusions

The proliferation of Web 2.0 has sparked the rapid rise of social networks. Concurrently, information privacy issues in social networks continue to dominate ongoing discussions on the consequences they have on users (Forbes, 2011). The outcomes of this research have advanced the existing knowledge concerning UIPC, potent antecedents, and PPB in the social network-mediated environment. The research empirically establishes that SN users who are concerned with their information privacy adopt PPB to safeguard their privacy. Moreover, it is noteworthy that UIPC are a strong predictor of PPB in SNs.

In the first place, the present research investigated five potent antecedents of UIPC in SN. The results confirm that three out of the five antecedents significantly contributes to UIPC. Specifically, perceived severity influences UIPC that connote users' perception of negative consequences of information privacy risks in SNs (e.g., identity theft), which compels them to adopt PPB as a precautionary measure. This reflects prior studies on behavioral intention to adopt virus protection (Lee, LaRose, & Rifon, 2008) and anti-spyware measures (Chenoweth, Minch, & Gattiker, 2009). Perceived vulnerability contributes the maximum (according to beta weights) towards UIPC. This implies that users

**Table 8.** Inference drawn on hypotheses.

Hypotheses	Structural relationships	Beta coefficient	t-value	Results
H1	UIPC $\rightarrow$ PPB	0.514	9.896**	Supported
H2	Perceived severity $\rightarrow$ UIPC	0.262	3.206*	Supported
H3	Perceived vulnerability $\rightarrow$ UIPC	0.447	6.724**	Supported
H4	Response efficacy $\rightarrow$ UIPC	0.027	0.768	Not Supported
H5	Rewards $\rightarrow$ UIPC	-0.014	-0.384	Not Supported
H6	Self-efficacy $\rightarrow$ UIPC	0.259	4.848**	Supported

Note. \* $p \leq 0.05$ ; \*\* $p \leq 0.001$ .

who believe that information security risks might occur are highly concerned about their information privacy in SNs. Accordingly, they exhibit PPB to safeguard themselves from potential security risks in SNs. This empirical finding is similar to prior studies on consumers' perception regarding online fraud (Crossler, 2010) and the prime reason for data backup (Larose & Rifon, 2007). The relationship between self-efficacy and UIPC was found to be positive and significant. This result implies that users who possess the confidence and ability to protect themselves from privacy threats have concerns with UIPC, which, in turn, drives them to exercise PPB in SNs. Following this logic, users who believe that they do not have the ability to protect themselves may be least concerned with their information privacy. Hence, our finding seems consistent with what has been reported in the pertinent literature (Chai et al., 2009; Mohamed & Ahmad, 2012).

The interesting finding of the present research deals with the insignificant effects of response efficacy and rewards towards UIPC. In this regard, response efficacy did not significantly contribute to UIPC. This implies that users' belief regarding protective measures in coping with information privacy threats in SNs does not essentially influence UIPC. This finding contradicts the existing literature (Phelps, Nowak, & Ferrell, 2000; Woon, Tan, & Low, 2005).

A possible explanation for this contradiction may be interpreted by considering the fact that users' past experiences shape their thought process and behaviors (Umeh, 2004). Following this logic, respondents had little prior experience of personal information misuse; therefore, it did not influence their coping behavior (i.e., response efficacy). Additionally, respondents may have perceptions that they are less vulnerable to risks as compared to their peers. Apart from response efficacy, linkage between rewards and UIPC was not found to be statistically significant. This finding implies that exciting benefits related with compromising personal information in SN are immaterial to UIPC. However, the finding does not fall in line with prior studies (Zhmag & McDowell, 2009; Crossler, 2010). One plausible explanation can be that respondents perceived rewards in monetary and non-monetary terms. The present study explored rewards in the context of SN, focusing primarily on intangible benefits (e.g., sense of connectedness); therefore, rewards did not show a significant influence on UIPC. However, monetary rewards have been found to significantly affect

privacy concerns and online behavior (Xie, Teo, & Wan, 2006).

### Theoretical, managerial, and social implications

The study was based on the following research questions: (a) Do UIPC directly influence PPB in social networks? (b) What are the antecedents of UIPC in social networks?

The Internet has given rise to the widespread usage and growth of SNs. Nowadays, SNs have exceeded the boundaries of just a platform for interaction and maintaining relationships. People are using social networks for even the smallest of things; they have become an inevitable part of daily life. However, the social networking environment cannot escape the aspect of risks. Users are often jeopardized by privacy threats, inappropriate utilization of personal information, identity thefts, phishing, and many others. The findings suggest that users assess the privacy risks and are cognizant of the protection mechanisms available in SNs.

The conceptual understanding of this research study was developed through PMT and SCT. According to the findings, users having information privacy concerns will mostly incorporate protection behavior in SNs. Interestingly, only perceived vulnerability, perceived severity, and self-efficacy were found to be significant predictors of UIPC in SNs. Compared to prior researchers who applied SCT and PMT, this study did not find empirical support for the relationship of rewards and response efficacy towards UIPC in SNs. This suggests that users' beliefs regarding protective action to cope with information privacy threats do not pertain to their privacy concerns. Moreover, exciting benefits linked to sharing personal information in social networks are linked to users' privacy concerns. Hence, this research contributes to the existing literature in the social networking context by manifesting that both PMT and SCT adequately explain UIPC in SNs. The research also offers a methodological contribution by validating the research instrument adapted from earlier studies in Indian settings. Consequently, this instrument may assist academic researchers and practitioners to elicit users' perceptions of privacy risks, information privacy concerns, and privacy protection behavior in social networks.

From a managerial perspective, the findings provide SN developers with an enhanced knowledge of how information privacy concerns significantly affect the



privacy protection behaviors of SN users. The privacy policies of the SN inevitably require continuous updating and monitoring to address these concerns. In addition, readability and visibility of SN privacy policies demand immediate improvement. Prior studies (Blatterer, 2010; Jeong & Kim, 2017) highlight that a majority of users do not read SN privacy policies. Accordingly, SN developers can formulate a summarized version of privacy policies that can assist users to realize the nature of personal information covered. For minimizing information privacy concerns, SN developers should understand the underlying factors that influence UIPC. The results of the present study indicate that perceived vulnerability contributes highly to UIPC, which implies that SN users feel at risk while providing their personal information. To deal with this situation of uncertainty, SN developers and operators should create stringent privacy mechanisms, thereby restricting the misuse of users' personal information by unauthorized parties. SNs can exercise greater control over information privacy by solely sharing users' personal information with trustworthy stakeholders (third parties, search engines, etc.) subject to the agreement of the user. Considering the societal angle, the findings of this study suggest that awareness about information privacy appears to be a grey area; therefore, regulatory bodies and policymakers should carry out specific initiatives to create awareness regarding online data privacy among the SN users. Further, this study can offer assistance to formulate policies for ensuring that SN developers and marketers are complying with ethical information-sharing practices and norms.

### Limitations and future research directions

As it is true for any empirical research, the current study also has limitations that warrant a careful and methodological interpretation of the results. First, the research was specifically conducted in the Indian context; therefore, the results cannot be generalized and might not hold true in the case of other countries. Future researchers should address this limitation by testing diverse samples from a cross-country perspective to empirically validate this study's findings. Second, even though the sample size used in the study was fairly large, it was mostly young adults; i.e., unidimensional. Despite variation in UIPC that exists among the respondents, it might not be sufficient to explain the

overall variance of the entire population base of SN users. Future research should possibly explore the role of age-group-related differences along with cultural variations, to exhibit the potential interaction effects of these two elements. Third, the study mainly focused on assessing the impact of UIPC on PPB in social networks in general. Future studies should investigate the proposed relationships for specific social networks (e.g., Facebook, Twitter, etc.), which might yield valuable insights for SN providers, marketers, and other parties. Lastly, the authors recommend conducting qualitative interviews and focus-group discussions of SN users to effectively understand the dynamic nature of UIPC.

### ORCID

Kishalay Adhikari  <http://orcid.org/0000-0002-6528-1320>

### References

- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. In G. Danezis & P. Golle (Eds.), *Privacy enhancing technologies* (pp. 36–58). Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag.
- Akhter, S. H. (2014). Privacy concern and online transactions: The impact of Internet self-efficacy and Internet involvement. *Journal of Consumer Marketing*, 31(2), 118–125. doi:10.1108/JCM-06-2013-0606
- Altman, I. (1975). *The environment and social behavior: Privacy personal space territory crowding*. Monterey, CA: Brooks/Cole.
- Anderson, J. C., & Gerbing, W. D. (1988). Structural equation modelling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103(3), 411–423. doi:10.1037/0033-2909.103.3.411
- ASSOCHAM Mahindra-SSG Report. (2015). *Cyber and network security framework*. Retrieved from <http://www.assocham.org/newsdetail.php?id=4821>
- Awwal, M. A. (2011). *An empirical investigation of the relationship between computer self-efficacy and information privacy concerns* (Doctoral dissertation). Nova Southeastern University, Ft. Lauderdale, FL, USA.
- Bandura, A. (1986). *Social foundations of thought and action*. Englewood Cliffs, NJ: Prentice-Hall.
- Bandura, A. (1989). Regulation of cognitive processes through perceived self-efficacy. *Developmental Psychology*, 25(5), 729–735. doi:10.1037/0012-1649.25.5.729
- Bandura, A. (1995). *Self efficacy in changing societies*. Cambridge, England: Cambridge University Press.
- Baren, J. V., Ijsselstein, W., Romero, N., Markopoulos, P., & Ruyter, B. (2003, October). *Affective benefits in communication: The development and field-testing of a new*



- questionnaire measure. Paper presented at the PRESENCE, Aalborg, Denmark.
- Basak, E., & Calisir, F. (2015). An empirical study on factors affecting continuance intention of using Facebook. *Computers in Human Behavior*, 48, 181–189. doi:10.1016/j.chb.2015.01.055
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1042. doi:10.2307/41409971
- Big Brother Watch. (2013). *New research: Global attitudes to privacy online*. Retrieved from <https://bigbrotherwatch.org.uk/2013/06/new-research-global-attitudes-to-privacy-online/>
- Blatterer, H. (2010). Social networking, privacy, and the pursuit of visibility. In H. Blatterer, P. Johnson, & M. Markus (Eds.), *Modern privacy: Shifting boundaries, new forms* (pp. 73–87). New York, NY: Palgrave Macmillan.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837–864. doi:10.25300/MISQ/2015/39.4.5
- Burcu, B., Cavusoglu, H., & Benbasat, I. (2010). Understanding emergence and outcomes of information privacy concerns: A case of Facebook. *Proceedings of the 31st International Conference on Information Systems (ICIS 2010)*, St. Louis, MO, USA (December 12–15, 2010).
- Business Insider. (2015). *Here's how much time people spend on Facebook per day*. Retrieved from <https://www.businessinsider.in/Heres-how-much-time-people-spend-on-Facebook-per-day/articleshow/47995030.cms>
- Byrne, B. M. (2010). *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming*, 2nd ed. (Multivariate Applications Series), New York: Routledge.
- Byrne, B. M. (2016). *Structural Equation Modeling With AMOS: Basic Concepts, Applications, and Programming*, Third Edition (Multivariate Applications Series), NY: Routledge.
- Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, 52(2), 167–182. doi:10.1109/TPC.2009.2017985
- Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). *Application of protection motivation theory to adoption of protective technologies*. Paper presented at the 42nd Hawaii International Conference on System Sciences, Honolulu, HI.
- Cho, H. (2010). Determinants of behavioral responses to online privacy: The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. *Journal of Information Privacy and Security*, 6(1), 3–27. doi:10.1080/15536548.2010.10855879
- Chu, S. C., & Choi, S. M. (2011). Electronic word-of-mouth in social networking sites: A cross-cultural study of the United States and China. *Journal of Global Marketing*, 24(3), 263–281. doi:10.1080/08911762.2011.592461
- Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly*, 23(2), 145–158. doi:10.2307/249749
- Crossler, R. E. (2010, January). *Protection motivation theory: Understanding determinants to backing up personal data*. Paper presented at the 43rd Hawaii International Conference on System Sciences, Honolulu, HI.
- Craighead, C. W., Ketchen, D. J., Dunn, K. S., & Hult, G. T. M. (2011). Addressing common method variance: guidelines for survey research on information technology, operations, and supply chain management. *IEEE Transactions on Engineering Management*, 58(3), 578–588.
- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3), 285–297.
- Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents: Measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), 413–422. doi:10.1002/ejsp.2049. doi:10.1080/01449290410001715723
- Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior*, 33, 153–162. doi:10.1016/j.chb.2014.01.009
- Forbes. (2011). *Facebook's Privacy Issues Are Even Deeper Than We Knew*. Retrieved from <https://www.forbes.com/sites/chunkamui/2011/08/08/facebooks-privacy-issues-are-even-deeper-than-we-knew/#644a31951421>
- Fornell, C. G., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. doi:10.2307/3151312
- Grindley, E. J., Zizzi, S. J., & Nasypany, A. M. (2008). Use of protection motivation theory, affect, and barriers to understand and predict adherence to outpatient rehabilitation. *Physical Therapy*, 88(12), 1529–1540. doi:10.2522/ptj.20070076
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2012). *Multivariate Data Analysis*, 7th ed., Upper Saddle River, NJ: Pearson Prentice Hall.
- Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate data analysis: A global perspective* (Vol. 7). Upper Saddle River, NJ: Pearson Education.
- Harman, H. H. (1976). *Modern factor analysis*. Chicago, IL: University of Chicago Press.
- Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 37(1), 275–298. doi:10.25300/MISQ/2013/37.1.12
- Hsu, M. H., Ju, T. L., Yen, C. H., & Chang, C. M. (2007). Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies*, 65(2), 153–169. doi:10.1016/j.ijhcs.2006.09.003

- Hudson, S., Huang, L., Roth, M. S., & Madden, T. J. (2016). The influence of social media interactions on consumer-brand relationships: A three-country study of brand perceptions and marketing behaviors. *International Journal of Research in Marketing*, 33(1), 27–41. doi:10.1016/j.ijresmar.2015.06.004
- Ijsselstein, W., van Baren, J., Markopoulos, P., Romero, N., & De Ruyter, B. (2009). Measuring affective benefits and costs of mediated awareness: Development and validation of the ABC-Questionnaire. In P. Markopoulos, B. De Ruyter, & W. Mackay (Eds.), *Awareness systems* (pp. 473–488). London, England: Springer-Verlag.
- Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior*, 69, 302–310. doi:10.1016/j.chb.2016.12.042
- Kansal, P. (2014). Online privacy concerns and consumer reactions: Insights for future strategies. *Journal of Indian Business Research*, 6(3), 190–212. doi:10.1108/JIBR-06-2012-0046
- Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, 48(4), 15–24.
- Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109–125. doi:10.1057/jit.2010.6
- Kumar Mishra, M., Kesharwani, A., & Das, D. (2016). The relationship between risk aversion, brand trust, brand affect and loyalty: Evidence from the FMCG industry. *Journal of Indian Business Research*, 8(2), 78–97.
- Lanier, C. D., & Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review*, 12(2), 1–49.
- LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, 41(1), 127–149. doi:10.1111/j.1745-6606.2006.00071.x
- LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005, May). *Online safety strategies: A content analysis and theoretical assessment*. Paper presented at the 55th Annual Conference of the International Communication Association, New York, NY.
- Lee, D., LaRose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445–454.
- Lee, T. S., Kilbreath, S. L., Sullivan, G., Refshauge, K. M., & Beith, J. M. (2007a). The development of an arm activity survey for breast cancer survivors using the Protection Motivation Theory. *BMC Cancer*, 7(1), 75. doi:10.1186/1471-2407-7-75
- Lee, Y., Lee, J. Y., & Liu, Y. (2007b). *Protection motivation theory in information system adoption: A case of anti-plagiarism system*. Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007), Keystone, CO (August 9–12, 2007), 62.
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394–413.
- Lim, J. S., Heinrichs, J. H., & Lim, K. S. (2017). Gender and hedonic usage motive differences in social media site usage behavior. *Journal of Global Marketing*, 30(3), 1–13. doi:10.1080/08911762.2017.1308615
- Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86(1), 114–121.
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. doi:10.1016/0022-1031(83)90023-9
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355. doi:10.1287/isre.1040.0032
- Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), 15–29.
- Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3), 449–473. doi:10.1111/j.1745-6606.2009.01148.x
- Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, 7(2), 163–184. doi:10.1348/135910702169420
- 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. doi:10.1016/j.chb.2012.07.008
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). New York, NY: McGraw-Hill.
- Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Which factors explain employees' adherence to information security policies? An empirical study*. Proceedings of the Pacific Asia Conference of the Information Systems, Auckland, New Zealand (July 4–6, 2007).
- Panek, E. T., Nardis, Y., & Konrath, S. (2013). Mirror or megaphone? How relationships between narcissism and social networking site use differ on Facebook and Twitter. *Computers in Human Behavior*, 29(5), 2004–2012. doi:10.1016/j.chb.2013.04.012
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27–41. doi:10.1509/jppm.19.1.27.16941
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903. doi:10.1037/0021-9010.88.5.879

- Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research*, 11(3), 153–161. doi:10.1093/her/1.3.153
- Raschke, R. L., Krishen, A. S., & Kachroo, P. (2014). Understanding the components of information privacy threats for location-based services. *Journal of Information Systems*, 28(1), 227–242. doi:10.2308/isis-50696
- Reid, M., & Levy, Y. (2008). Integrating trust and computer self-efficacy with TAM: An empirical assessment of customers' acceptance of banking information systems (BIS) in Jamaica. *Journal of Internet Banking and Commerce*, 12(3), 1–17.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. doi:10.1080/00223980.1975.9915803
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). New York, NY: Guilford Press.
- Schwarzer, R., & Renner, B. (2000). Social-cognitive predictors of health behavior: Action self-efficacy and coping self-efficacy. *Health Psychology*, 19(5), 487–495. doi:10.1037/0278-6133.19.5.487
- Searle, A., Norman, P., Harrad, R., & Vedhara, K. (2002). Psychosocial and clinical determinants of compliance with occlusion therapy for amblyopic children. *Eye*, 16(2), 150–155. doi:10.1038/sj/eye/6700086
- Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising*, 28(3), 37–51. doi:10.1080/00913367.1999.10673588
- Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62–73. doi:10.1509/jppm.19.1.62.16949
- Sheeran, P., Harris, P. R., & Epton, T. (2014). Does heightening risk appraisals change people's intentions and behavior? A meta-analysis of experimental studies. *Psychological Bulletin*, 140(2), 511–543. doi:10.1037/a0033065
- Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, 22(5), 428–438. doi:10.1016/j.intcom.2010.05.001
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196. doi:10.2307/249477
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1016. doi:10.2307/41409970
- Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32(2), 503–529. doi:10.2307/25148854
- Soper, D. S. (2015). A-priori sample size calculator for structural equation models [Software]. Available from <http://www.danielsoper.com/statcalc>
- Statista. (2016). *India: Number of Facebook users in India from 2015-2022*. Retrieved from <https://www.statista.com/statistics/304827/number-of-facebook-users-in-india/>
- Sung, Y., Kim, Y., Kwon, O., & Moon, J. (2010). An explorative study of Korean consumer participation in virtual brand communities in social network sites. *Journal of Global Marketing*, 23(5), 430–445. doi:10.1080/08911762.2010.521115
- Umeh, K. (2004). Cognitive appraisals, maladaptive coping, and past behaviour in protection motivation. *Psychology & Health*, 19(6), 719–735. doi:10.1080/0887044042000196692
- VentureBeat. (2016). *Facebook passes 1.65 billion monthly active users, 54% access the service only on mobile*. Retrieved from <https://venturebeat.com/2016/04/27/facebook-passes-1-65-billion-monthly-active-users-54-access-the-service-only-on-mobile/>
- Van De Garde-Perik, E., Markopoulos, P., De Ruyter, B., Eggen, B., & Ijsselstein, W. (2008). Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review*, 26(1), 20–43. doi:10.1177/0894439307307682
- Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 36(4), 531–542. doi:10.1016/j.ijinfomgt.2016.03.003
- Woon, I., Tan, G. W., & Low, R. (2005). *A protection motivation theory approach to home wireless security*. Proceedings of the 26th International Conference on Information Systems, Las Vegas, NV (December 11–14, 2015), 367–380.
- Xie, E., Teo, H. H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters*, 17(1), 61–74. doi:10.1007/s11002-006-4147-1
- Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). *Examining the formation of individual's information privacy concerns: Toward an integrative view*. Proceedings of 29th International Conference on Information Systems, Paris, France (December 14–17, 2008), 1–16.
- Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86–110. doi:10.1207/s15506878jobem4901\_6
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), 389–418.
- Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, 16(4), 479–500. doi:10.1080/1369118X.2013.777757
- Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3–4), 180–197. doi:10.1080/15332860903467508