Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks: Evidence from India

Kishalay Adhikari[1], Doctoral Scholar,
Dr. Rajeev Kumar Panda[2], Assistant Professor
School of Management, National Institute of Technology, Rourkela

Abstract

Purpose: This research aims to understand the impact of antecedents of users' information privacy concerns (UIPC) on privacy protection behavior (PPB) in social networks.

Design Methodology Approach: The conceptualization of the research model is grounded in the Social Cognitive and Protection Motivation theories. Survey questionnaires were used to collect empirical data from 337 university students; out of which 306 samples were included in analyses. The proposed research model was analyzed using structural equation modelling technique in SPSS AMOS 20.

Findings: Perceived vulnerability, perceived severity and self-efficacy were found to be significantly affecting UIPC. However, Rewards and response efficacy did not contribute to UIPC. The linkage between UIPC and PPB was found to be statistically significant.

Implications: This empirical study will offer newer insights into the existing theoretical foundations of privacy in the context of social networks. Also, the findings will assist the social networking website providers to develop and implement privacy protection strategies to safeguard the users from privacy threats.

riginality Value: Since last decade, the rapid growth of social networks has raised serious concerns in terms of breach of privacy. The present research makes a novel attempt to provide empirical evidence of the relationship between UIPC and PPB in the Indian context. Hence, it tries to bridge the gap between theoretical and practical aspects of information privacy.

ey ords: Social networks, Information privacy, Privacy protection, Social Cognitive Theory, Protection Motivation Theory

USERS' INFORMATION PRIVACY CONCERNS AND PRIVACY PROTECTION BEHAVIOUR IN SOCIAL NETWORKS: EVIDENCE FROM INDIA

Presented by:

Dr. Rajeev Kumar Panda and Kishalay Adhikari

School of Management, NIT Rourkela, Odisha-769008

(IIM-NASMEI MARCON, 29th July 2017)

Criticality of the issue- *Privacy in virtual spaces*

"Even if information privacy is claimed, it cannot be a fundamental right"

(Argument of Attorney General K.K. Venugopal in front of nine-judge bench headed by Chief Justice J.S. Khehar).

- Supreme court has already delivered two judgments in 1950 and 1962 stating privacy is not a fundamental right.
- 94% Indians are concerned with their online privacy, as reported in a research conducted by ComRes (2013) involving 10,354 online users from nine countries.
- During 2011-2015, over half million Indians' have been victims of privacy intrusions i.e. their personal information was compromised (ASSOCHAM-Mahindra SSG report, 2015).

Theoretical background

- ***Information privacy concerns***: Extent to which an individual is concerned about organizational practices related to the collection and use of his/her personal information (Smith, Milberg, & Burke, 1996).

- ***Protection motivation theory:*** Suggests that risks and benefits are essential factors necessary to explain how people manage behavior in risky situations (Youn, 2005). The paramount assumption of the theory is that individuals are motivated to protect themselves if they feel threatened in risky events (Youn, 2005).

- ***Social Cognitive theory***: Human behavior is dynamic and mutual interaction of personal, behavioral, and environment factors (Bandura, 1989).

Breakthrough Studies

Researcher and year	Findings
Altman (1975)	Initially explored the linkage between privacy concerns and protection behaviour and suggested, *''People attempt to implement desired levels of privacy by using behavioural mechanisms…"*
Dinev and Hart (2004)	Perceived vulnerability and Perceived ability to control substantially explains individuals' information privacy concerns.
Malhotra et al. (2004) and Smith et al. (2011)	Online privacy concerns significantly influences perceived trust and risk notions.
Acquisti and Gross (2006); Shin (2010); Tucker (2014)	Rich application of privacy in social network context argues they offer interesting features to lure individuals, yet suffer from security threats, weak access controls, and feeble design.

Breakthrough Studies

Researcher and year	Findings
Jones et al. (2004); Young and Quan-Haase (2013); Feng and Xie (2014)	In virtual spaces, privacy concern is an ethical issue since online companies are dependent on the collection and storage of users' personal info. in their databases. Subsequently, this enhances users' concerns as their personal info. can be compromised.
Son and Kim (2008); Wang et al. (2016)	Info. privacy concerns positively and significantly influence willingness to online info. disclosure.
Rogers (1975, 1983); Youn (2005)	PMT theory considers risks and benefits as crucial factors in explaining individual behaviour in high-risk situations. Major components of PMT- perceived vulnerability, perceived severity, response efficacy, self- efficacy, rewards, and response costs.
Aimeur et al. (2010)	Privacy measures are too stringent to guarantee sufficient protection to users.

Research Gap

- Despite the advancement in the conceptual (Dinev and Hart, 2004; Shin, 2010; Qi and Edgar-Nevill, 2011) and empirical (Smith et al., 2011; Hong and Thong, 2013; Tucker, 2014) treatment of information privacy concerns, the understanding of this important construct remains partial.

- The majority of research published on information privacy concerns are limited to "Euro-American" context with the exception of a few notable studies investigating this construct in emerging countries.

- PMT studies have focused on two prime areas-health studies and IS research (Lee *et al*., 2007a, 2007b). Empirical support for the application of PMT in the context of social networks, however, is not clearly evident.

Proposed Hypotheses

Hypothesis 1: *PS positively and significantly influences UIPC in social networks*

Hypothesis 2*: PV positively and significantly influences UIPC in social networks*

Hypothesis 3: *REW negatively and significantly influences UIPC in social networks*

Hypothesis 4: *RE positively and significantly influences UIPC in social networks*

Hypothesis 5: *SE positively and significantly influences UIPC in social networks*

Hypothesis 6: *UIPC positively and significantly related to PPB in social networks*

Methodology

- **Sampling technique:** Snowball and Convenience sampling (Non-probability sampling approach)
- **Scale development:** Adapted and modified from prior researchers [Dinev & Hart (2004), Milne & Culnan (2004), Woon et al. (2005), Larose & Rifon (2007), Lee et al. (2008), Youn (2009), Crossler (2010)]
- **Data collection:** Online survey questionnaires was used for gathering responses. 337 responses were received in total, 31 responses were eliminated due to high missing values.
- **Data Analysis:** Data was analyzed using SPSS 20 and AMOS package 20 and the tools such as descriptive statistics, exploratory factor analysis, and structural equation modeling to draw meaningful insights.

Reliability & validity measures

Construct	*Cronbach a*	*CR*	*AVE*
PS	0.840	0.841	0.571
PV	0.860	0.861	0.675
REW	0.842	0.849	0.654
RE	0.781	0.783	0.547
SE	0.883	0.885	0.721
UIPC	0.908	0.910	0.670
PPB	0.916	0.915	0.644

	PS	SE	REW	PV	RE	UIPC	PPB
PS	**0.755**						
SE	0.370	**0.849**					
REW	0.015	0.056	**0.809**				
PV	0.409	0.450	0.098	**0.822**			
RE	0.126	0.168	0.037	0.038	**0.739**		
UIPC	0.463	0.522	0.027	0.614	0.079	**0.819**	
PPB	0.294	0.503	0.194	0.490	0.121	0.551	**0.802**

Threshold values: AVE ≥ 0.5, CR ≥ 0.7, Cronbach α ≥ 0.7 [Fornell & Larcker (1981), Nunnally & Bernstein (1994), Hair et al. (2010)]
Diagonal values in bold indicates squared root estimate of AVE (**Discriminant validity**)

Common method bias assessment

Harman's single factor test (using CFA)

Model-fit Indices	*Multi-factor Model*	*Single-factor Model*	*Difference* (Δ)
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

Common method bias assessment (contd.)

Unmeasured Latent Construct Method

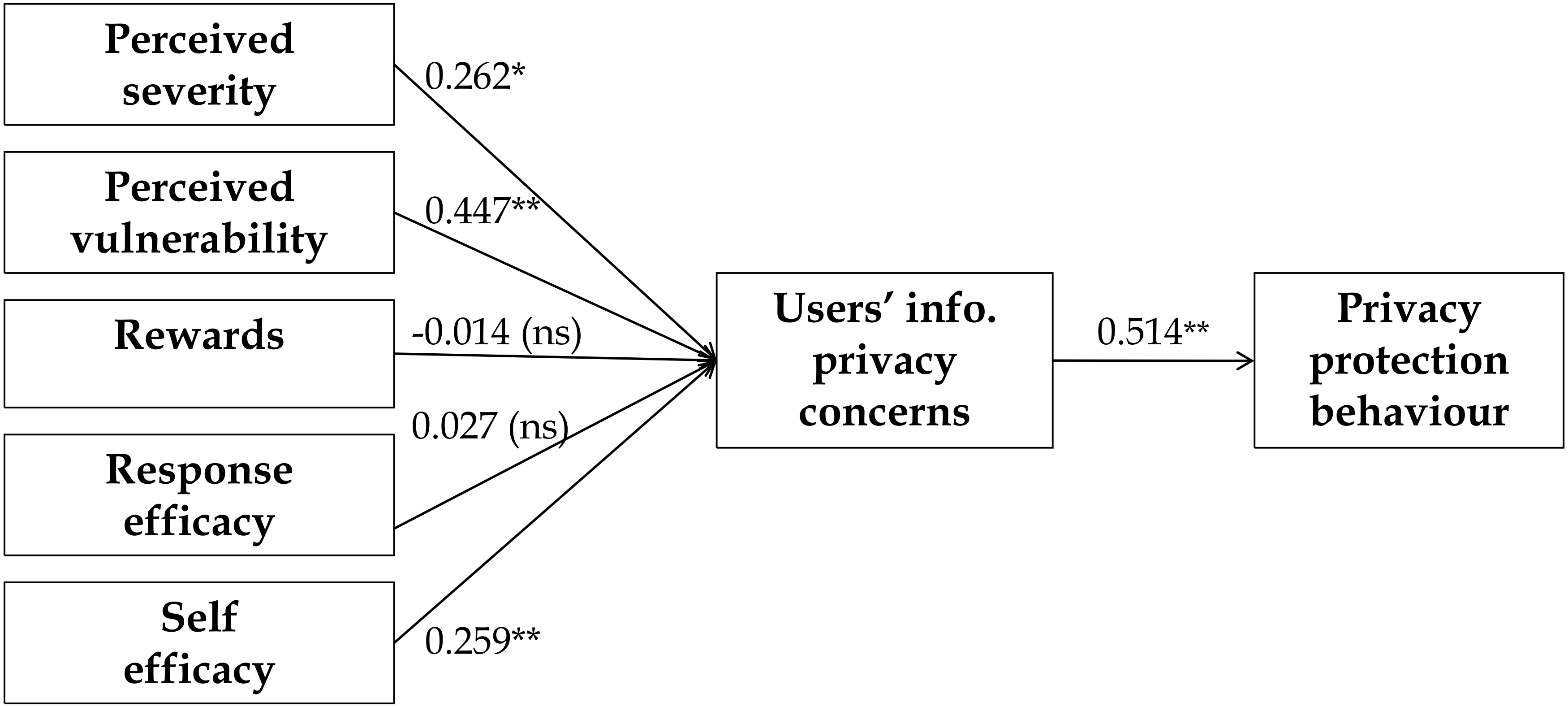
Measurement item	Standardized Estimates (With CLF)	Standardized Estimates (Without CLF)	Δ
PS1	0.750	0.756	0.006
PS2	0.647	0.656	0.009
PS3	0.781	0.804	0.023
PS4	0.796	0.805	0.009
PV1	0.730	0.749	0.019
PV2	0.772	0.848	0.076
PV3	0.815	0.863	0.048
REW1	0.743	0.744	0.001
REW2	0.748	0.759	0.011
REW3	0.905	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

Measurement item	Standardized Estimates (With CLF)	Standardized Estimates (Without CLF)	Δ
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

Measurement and structural model fit-indices

Fit Index	*Recommended Value*	*Measurement Model*	*Structural Model*
CMIN/df (Chi-square; df)	≤ 3	1.624 (492.217; 303)	1.637 (500.840;306)
CFI	≥ 0.90	0.96	0.959
GFI	≥ 0.80	0.896	0.894
AGFI	≥ 0.80	0.870	0.869
NFI	≥ 0.90	0.904	0.902
IFI	≥ 0.90	0.961	0.960
RMSEA	≤ 0.08	0.045	0.046

Structural Model Results



Notes: significant at $*p < 0.05$; $**p < 0.01$

Inference drawn on hypotheses

Hypotheses	*Relationship*	*Path estimates*	*t-value*	*Decision*
H1	PS → UIPC	0.262	3.206*	Supported
H2	PV → UIPC	0.447	6.724**	Supported
H3	REW → UIPC	-0.014	-0.384	Not Supported
H4	RE → UIPC	0.027	0.768	Not Supported
H5	SE → UIPC	0.259	4.848**	Supported
H6	UIPC → PPB	0.514	9.896**	Supported

Implications for theory and practice

- The present research provides theoretical justification, as well as empirical evidence, in support of the conceptual links between UIPC, its antecedents, and PPB. The findings of this research manifest both PMT & SCT theories adequately explain UIPC in social networks in Indian context.

- This research assist academicians regarding means and ways to tackle common method bias, which may dilute the results; in conducting various research studies.

- From a managerial perspective, this research would aid the social network providers to redesign their privacy mechanisms.

- Based on the insights offered, social network providers and the govt. policymakers may undertake informative programs to raise awareness about privacy issues in social networks.

Limitations and avenues for future research

- This 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.

- Unidimensionality of sample [majorly college-going students (18-25 years)] may introduce measurement bias into the research data. Hence, future researchers can investigate this issue by considering other age-groups or multi age-groups.

- The study mainly focused on examining the impact of UIPC on PPB. In this regard, we did not examine the different sources of UIPC. Additional research can yield valuable insights by exploring this construct in the social networking settings.

- Future researchers may conduct longitudinal studies to effectively understand the dynamic nature of information privacy.

Thank you everyone