(IJTBM) 2018, Vol. No.8, Issue No. IV, Oct-Dec e-**ISSN: 2231-6868, p-ISSN: 2454-468X**

SOCIAL NETWORKING SITE AND PRIVACY- IDENTIFYING THE KEY INFLUENCERS WIZ.DEMOGRAPHICS, SOCIAL PREFERENCES TO DEVELOP A MODEL TO ENHANCE THE EFFICACY OF DATA PRIVACY

Ashima Jindal
Presidium School
Ashok Vihar, Delhi

ABSTRACT

The purpose of this paper is to propose and examine a privacy behaviour model within the context of Social networking factors (Indian scenario). The results of the key components of SNS factors on perceived values of privacy behaviour were by trial and error determined. SNS is conceptualized as a multi-dimensional construct as well as emotional privacy, social privacy, personal privacy, and value. The investigated socio-demographic factors enclosed, age, gender, ethnicity, education level, financial gain level, and components of SNS from that sometimes impacts the privacy behavior. the first knowledge was gathered by a form survey of online users. mistreatment 323 survey returns, correlational analysis, and Z check analysis were utilized for knowledge analysis and hypothesis testing. The projected model was tried valid and also the 5worth constructs cumulatively accounted for seventy.2% of the variance in SNS for privacy behaviour. Social media parameters and Privacy scams considerably affected perceived social and emotional privacy behaviour. on-line advantages and Legal structure considerably affected all perceived individual privacy considerations. Incorporation of emotional privacy, social privacy, personal privacy, and worth kind info in developing SNS promoting ways and promotional programs will facilitate firms a lot of effectively convey desired values of privacy to focus on customers. This empirical study knowledgeable the necessity for the higher understanding of client privacy behaviour for SNS to support the simpler development and promoting. The information gained from this study provides valuable insights for each academician and industrial practitioners.

***KEYWORDS**: Privacy, Social media, User attitude, online networking, Social networking sites.*

I. INTRODUCTION

The usage of Social systems administration destinations for educational and socialization intentions is maybe associated with the use of a secretive profiles and customers enlivened by online long range informal communication's open estimations simply more viably adjust security settings (Xu, Luo, Carroll, and Rosson., 2011). The electronic person to person communication showed a productive association between the presentation of individual information and customers' number of mates and a negative connection between the usage of security settings and

the use of internet systems administration to meet new people, suggesting that protection practices may be related to social fulfillments (Culnan and Armstrong, 1999). The association among security and sociality is extremely flighty. While positive associations exist between the use of security controls and social capital results, security demeanors maycompel online networking exposure and contrarily affect the gathering of social capital advantages (Krasnova,Spiekermann, Koroleva, & Hildebrand, 2010). Customers see it essential to exchange singular information to recognize social targets and accomplish the social capital favorable circumstances that web based systems administration offer and that the risk ofunintended revelation is relieved by the social comfort for social administration (Boyd & Ellison, 2008).Customers of online informal communication indicate strong stresses over security on the web, yet routinely don't take an interest in protection guaranteeing hones, for instance, altering security controls, restricting revelation of geo zone information, or changing starting protection choices after framework advancement. The conspicuous legitimate irregularity between security tendencies and protection guaranteeing practices has confounded masters, and has been respected the security (Rosen, 2001). As a customer centered methodology, the uses and joys perspective offers information to appreciate web based systems administration use, and additionally how electronic person to person communication utilize is affected by protection concerns and how its usage may affect common security. Security stresses as being both social and institutional and related to informational introduction on casual network goals) (Karyda, Gritzalis, Stop, and Kokolaki, 2009). As the two basic zones for security concern, Information Control looks at to the social parts of enlightening presentation, while Power Loss relates dictator and institutional measurements. PersonalityLoss and Future Life of Information have likewise been perceived in earlier work, as "saw harm" and "sawprobability" of mischief, predecessors to worry about security. Essentially, this examination distinguished thesupremacy of Identity Loss and Future Life of Information as requested privacy concerns. This examination also demonstrated that security practices take after a real model that mirror different leveled levels of online development (Li, Wang, Li, and Che, 2016). Customers may go in their protection rehearses, anyway this work also gives demonstrate that customers shield their security in the meantime at various levels. The stresses over the usage of character information and how substance will be dealt with later on may prompt more instrumental types of engagement with web-based social networkingstages (Cho, Lee, & Chung, 2010).The internet organizing security is found in the usage of Social Curation when electronic interpersonal interaction is used for Communication or Escape. Relationship enhancement from the shallow to more close to home structures is as often as possible delineated as a method of self-introduction in which the weight of security control and the cheerfulness of the social setting feature dominatingly (Christofides, Muise, and Desmarais, 2009). Social invasion theory and correspondence security organization speculation) underscore the congruity of socially arranged approaches to manage protection that centre on disclosure in unmediated associations. Intervened circumstances showing those relative sorts of point of confinement control shapes are rehearsed by means of online systems administration

media stages and fortifying the immensity of social procedures in security bearing structures. The internet organizing protection perceived in this examination offers verification of how the security peculiarity may continue surfacing (Awad and Krishnan, 2006). The inclination is related to a nonattendance of commitment of utilization level security organization gadgets. This is enduring with how progressing media use is depicted all around, lacking concerning deliberateness or conceivably attentiveness in regards to the medium/message. The habituation crosses with protection organization in manners that present the potential for separation between security concerns and security hones. In this way, this prompts a continued with a sign of the security problem, notwithstanding extended comprehension and innovation in web-based systems administration utilize (Hiller, Smith, &Bélanger, 2002).

II. OBJECTIVES OF THE STUDY

With introduction to the above data it could be identified examination in regards to be concerned for privacy andsecurity organization in the reference of Social media goals ought to be driven along these lines of research objective a sorted out study had been proposed to assemble information from legitimate Social media customers for responding following investigation targets:

1) Are there critical privacy administration measures among Social media locales?

2) To recognize the segments of protection conduct on Social media areas which impacts the customers' manner towards individual to individual correspondence goals?

III. RESEARCH METHODOLOGY

An examination design was used to accumulate data considering the ultimate objective to survey the level privacybehaviour of online networking clients, and to test the exploration theories laid out already. This examinationplanned to research the effect of privacy behaviour of clients' acknowledgment of online networking locales inindigenous habitat. A review poll was produced to gauge each of the builds contained in our investigation inquireabout model. Estimation of the factors for the builds in the exploration display was adjusted from the audit of thewriting. Every factor was estimated on a five-point Likert scale where 1 signifies "emphatically deviate" and 5signifies "firmly concur". A pilot survey was utilized to guarantee that the inspected factors are noteworthy to theclients of web-based social networking locales. In light of the outcomes from the pilot survey, alterations weremade to the survey. The closed poll was then flowed to online clients. Altogether, 357 overview polls were comeback from the review respondents. In the wake of screening out deficient reactions, the study yielded 323 usablereactions. Exhibit 1 and Exhibit 2 give the synopsis of respondents' statistic data and additionally their onlinenetworking destinations utilization behaviour.

Exhibit 1 *Demographic profile of the respondents*
[N=323]

Age	*Frequency*	*Gender*	*Frequency*	*Education*	*Frequency*
14-16	54	**Male**	185	Undergraduate	242
16-18	159	**Female**	138	Graduate	42
18-20	29			Post graduate	39
20-22	42				
22-24	34				
24-26	5				

Exhibit 2 *Social media profile of the respondents*
[N=323]

Social media accounts	*Frequency*	*Time on Social media*	*Frequency*	**Privacy setting: private info accessible to**	*Frequency*
Facebook	180	**0-30 mins**	101	**Friends only**	147
LinkedIn	62	**30-60 mins**	42	**Friends and their friends**	87
Twitter	29	**60-90 mins**	40	**Public**	66
Google+	19	**90-120 mins**	95	**I don't know**	23
Youtube	33	**<120 mins**	45		

Key research variables: Exhibit 3 explains the descriptive analysis of the identified variables which wereemployed for exploratory factor analysis. The variables with high mean values i.e. Social recognition (Mean=3.90), Information sold (Mean=3.76) and Urge of sharing data online (Mean=3.65) are considered to be mostimpactful variables for the viewer's response for the social media contents.

Exhibit 3 *Descriptive statistics of identified variables*

Variables	**Mean**	**Std Dev**	**Max.**	**Min.**	**Skewness**	**Kurtosis**
Information sold	3.76854	2.56225	5	1	0.62639	-2.40692
Privacy system	2.89020	2.57257	5	1	0.43298	-2.63428
Social recognition	3.90802	2.62399	5	1	0.30044	-2.62866
Commercial usage	2.20089	2.32226	5	1	2.27738	0.37403
Legislation	2.30860	2.52373	5	1	2.00423	-0.68082
Number of users	2.25233	2.35202	5	1	2.26682	0.29262
Urge of sharing data online	3.65608	2.42974	5	1	2.00988	-0.43266
Brand awareness	2.88724	2.03468	5	1	2.06466	-0.06442
Legal punishment	3.20772	0.58220	5	1	2.69806	6.06466
Ease of use	2.60237	2.53405	5	1	0.66380	-2.27426
Significance for privacy	2.28694	2.38575	5	1	2.22392	0.09068
Website structure	2.90802	2.28541	5	1	2.64669	2.82768
Certification of the site	3.38575	1.24146	5	1	-0.04268	-2.67074
Discounts	2.66272	1.50142	5	1	0.66422	-2.26696
User awareness	2.82899	1.29784	5	1	0.99748	-0.94269
Critical information leaked	2.43268	1.61234	5	1	0.59456	-0.70659
Code of conduct for data	2.64356	1.40987	5	1	0.45656	0.30163
Marketing of media	2.99976	1.20876	5	1	0.29875	-0.41642
Concessions	3.45789	1.26434	5	1	2.29876	-0.07653
Identity theft	2.22246	1.90765	5	1	2.04563	5.43556
Rewards	2.90854	1.54578	5	1	2.26788	-3.87642

IV. DATA ANALYSIS

Exploratory Factor Analysis: Principal component method with varimax rotations was used to reduce theproportions of model and to compress 21 classified variables identified under literature review. Kaiser-Meyer-Olkin (KMO) value of 0.83281975 in Exhibit 4 indicates sufficient number of items for each factor. Principalcomponent analysis employed to measure the degree of variability in the variables. The degree of variabilitycalculated from the initial value [=1], variables with extraction value more 0.5 would be considered acceptablefor factor analysis. Correlation matrix between test variables was significantly different from an identity matrix,in which correlations between variables are all zero. Eigen values greater than 1 were considered for factorextraction. It was found that total five factors with (Eigen value >1) accounts for 70.2% variance in all variablesconsidered for privacy concern.

Exhibit 4			***Kaiser's Measure of Sampling Adequacy: Overall MSA =*** **0.83281975**				
			***Final Communality Estimates: Total* = 15.1726**				
Info. . sold	*Privacy system*	*Social recognition*	*Commercial usage*	*Legislation*	*No. of Users*	*Urge of sharing*	*Brand awareness*
0.7723*	**0.7104***	**0.6892***	**0.7559***	**0.7898***	**0.6668***	**0.6287***	**0.7083***
Legal Punishment	*Ease of use*	*Sig. for privacy*	*Website structure*	*Certification of site*	*Discounts*	*User awareness*	*Critical info. leaked*
0.7354*	**0.5453***	**0.6254***	**0.8779***	**0.8307***	**0.6971***	**0.7359***	**0.6972***
Code of conduct for data	*Marketing of media*	*Concessions*	*Identity Theft*	*Rewards*			
0.7365*	**0.8234***	**0.6954***	**0.7523***	**0.6987***			
Initial value =1							
****= Extraction value***							***Extraction***
method= Principal Component analysis							

Exhibit 5 illustrates correlation between the each identified variables, the coefficient of correlation ranges between -1 to 1, and coefficient of correlation greater than 0.5 is considered as an acceptable correlation between thevariables.

V1= Information sold
V2= Privacy system leaked
V3= Social recognition
V4= Commercial usage
V5= Legislation
V6= Number of users
V7= Urge of sharing data online
V8= Brand awareness
V9= Legal punishment
V10= Ease of use
V11= Significance for privacy
V12= Website structure
V13= Certification of the site
V14= Discounts
V15= User awareness
V16= Critical information
V17 Code of conduct for data
V18= Marketing of media
V19= Concessions
V20= Identity theft
V21= Rewards

Exhibit 6 *Rotated Factor Pattern*

Variables	Factor1	Factor2	Factor3	Factor4	Factor5
Number of users	0.88740				
Privacy system	0.74752				
Website structure	0.72194				
Brand awareness	0.68786				
Ease of use	0.66415				
Marketing of media	0.63743				
Critical information leaked		0.86183			
Information sold		0.75462			
Identity theft		0.68020			
Commercial usage		0.53532			
Discounts			0.87794		
Social recognition			0.77922		
Concessions			0.68906		
Rewards			0.59876		
Legislation				0.83665	
Code of conduct for data				0.68432	
Certification of sites				0.62863	
Legal punishment				0.60232	
User awareness					0.77341
Urge to share data online					0.68432
Significance for piracy					0.59543

V. HYPOTHESIS AND THE PROPOSED MODEL

The key hypotheses proposed to be tested for the research are as follows:

H1: *Parameters of social media sites have a direct influence on a user's intent with respect privacy behaviouron social media sites.*

H2: *Privacy scams on social media sites have a direct influence on a user's intent with respect privacybehaviour on social media sites.*

H3: *Online benefits to the users have a direct influence on a user's intent with respect privacy behaviour onsocial media sites.*

H4: *Legal structure has a direct influence on a user's intent with respect privacy behaviour on social mediasites.*

H5: *User's attitude has a direct influence on a user's intent with respect privacy behaviour on social media sites.*

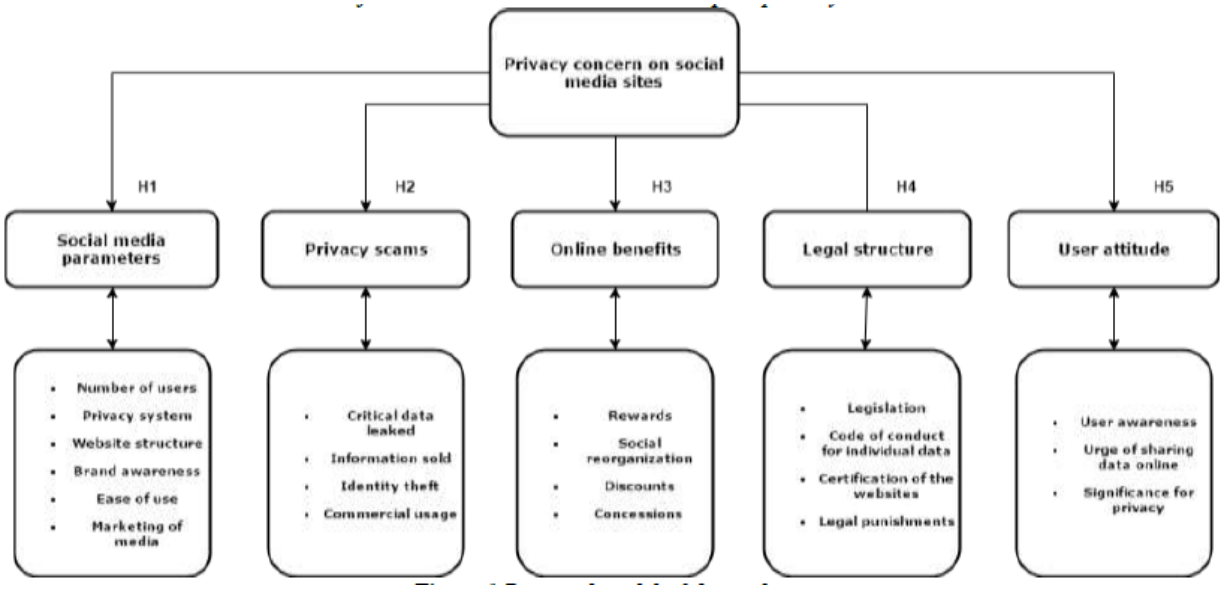

Figure 1 Proposed model of the study

Variable	DF	Parameter Estimate	Standard Error	Z Value	Pr > |t|
Intercept	1	1.55805	0.49222	4.65	0.0004
Social media site parameters	1	-0.52522	0.09294	-6.19	<.0001
Privacy scams on the website	1	-0.01890	0.12205	-0.15	<.0001
Online benefits	1	-0.01824	0.06266	-0.29	0.0214
Legal structure	1	0.48824	0.08950	5.45	<.0001
User's attitude	1	1.55805	0.49222	4.65	<.0001

Y= C+m1x1+m2x2+m3x3+m4x4+ m5x5

Predicted (Privacy behaviour on social media sites) = -1.55805+ (-0.52522*Social media site parameters) + (-0.01890* Privacy scams on the website) + (-0.01823* Online benefits) + (0.38823* Legal structure) + (1.55805* User attitude)

Analysis of Variance

Source	*DF*	*Sum of Squares*	*Mean Square*	*F Value*	*Pr > F*
Model	5	240.25408	24.02541	22.19	<.0001
Error	322	255.25692	0.85861	*Depd. Mean* 2.46000	**R-Square** 0.5525
Corrected Total	322	526.00000	*Root MSE* 0.92120	*Coeff Var* 53.29225	**Adj. R-Sq** 0.5558

Exhibit 7 *Results for privacy behaviour based on the identified variables*

VI. FINDINGS

The data gathered was normally distributed, as the data was checked for multicollinearity and heteroscedasticity.The 21 variables were identified and were used for exploratory factor analysis which was reduced to 5 factors byusing the Principal Component analysis and Varimax rotation method. The identified factors are as follows:

Factor 1 Social media parameters consists of variables Number of users, Privacy system, Website structure, Brandawareness, Ease of use and Marketing of media. *Factor 2* Privacy scam consists of variables Critical informationleaked, Information sold, Identity theft and Commercial usage. *Factor 3* Online benefit consists of variablesDiscounts, Social recognition, Concessions and Rewards. *Factor 4* Legal structure consists of variablesLegislation, Code of conduct for data, Certification of sites and Legal punishment. *Factor 5* User attitude consistsof variables User awareness, Urge to share data online and Significance for piracy. The results of data analysisare segmented into two sections. Section 1 consist of descriptive statistics of demographic and search engineprofile of the respondents and the majority of the respondents between the age of

20-25 years with graduate levelof education use Google as there prominent search engine for mostly 15 - 60 minutes in order to obtain updatesand information. Section 2 on other hand consists of Statistical and Hypothetical analysis of the identifiedvariables. Privacy behaviour with respect to SNS *(F value* 22.19 *and p value <.0001)* has significant impact onthe consumers. The most prominent elements of privacy behaviour identified in the research is it helps to socialmedia parameters *(p value =-0.619),* enhances the privacy behaviour of the user *(p value* = -0.15*)* followed byother factors i.e. Privacy scams.

VII. CONCLUSION

In view of the study results and hypothetical similar writing audit, organizations should know about the ramifications of privacy behaviour in SNS. There is growing evidence to suggest that younger people are moreconcern for privacy than was typical a generation ago. This provides opportunities and challenges for SNS tofocus on the grey market.

All of these conditions provide important insights into new patterns of consumer privacy behaviour for SNS torespond. The trend for younger consumers to have an increasing influence on the market place shows no signs ofslowing down. Being able to identify and communicate product benefits, which appeal to mature consumers,offers new challenges to the industry. Older consumers are more discerning about SNS attributes and respond tomarketing that reflects rather than compromises their key values. Limited research has been undertaken tocompare factors that affect why young users concern about privacy, how they behave, and what they set as theirprivacy, in relation to their age, gender and nationality. This research goes some way to address some of theseconcerns and begins the process of identifying key factors that need to be considered by SNS administrations andmarketers.

The survey data came from three different continents, thereby providing rich perspectives into globalconsumption. Companies who own domestic market share and want to enter new global markets could use thisdata to improve their product design development decisions.